Feyyat Kaymaz

User-Anonymität in Mobile Payment Systemen

Ein Referenzprozessmodell zur Gestaltung der User-Anonymität in Mobile Payment Systemen

kassel university press

Feyyat Kaymaz

User-Anonymität in Mobile Payment Systemen

Ein Referenzprozessmodell zur Gestaltung der User-Anonymität in Mobile Payment Sytemen

kassel university press

Die vorliegende Arbeit wurde vom Fachbereich Wirtschaftswissenschaften der Universität Kassel als Dissertation zur Erlangung des akademischen Grades eines Doktors der Wirtschafts- und Sozialwissenschaften (Dr. rer. pol.) angenommen.

Erster Gutachter: Prof. Dr. Udo Winand
Zweiter Gutachter: Prof. Dr. Gerd-Michael Hellstern

Tag der mündlichen Prüfung 6. Juli 2011

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar

Zugl.: Kassel, Univ., Diss. 2011
ISBN print: 978-3-86219-192-5
ISBN online: 978-3-86219-193-2
URN: http://nbn-resolving.de/urn:nbn:de:0002-31937

Umschlaggestaltung: Tove Günter, Düsseldorf
http://www.toveg.de/
Printed in Germany

I. Inhaltsübersicht

II. Inhaltsverzeichnis

III. Abkürzungsverzeichnis

Abs.	Absatz
AGB	Allgemeine Geschäftsbedingungen
AMPS	Advanced Mobile Phone Service
ANSI	American National Standards Institute
API	Application Programming Interface
Art.	Artikel
ASP	Application Service Provider
ATM	Automated Teller Machine
Aufl.	Auflage
Az.	Aktenzeichen
BDSG	Bundesdatenschutzgesetz
BMWA	Bundesministerium für Wirtschaft und Arbeit
BRD	Bundesrepublik Deutschland
B2C	Business to Consumer
BVerfG	Bundesverfassungsgericht
BvR	Bundesverfassungsrichter
BWL	Betriebswirtschaftslehre
bzw.	beziehungsweise
ca.	circa
C2C	Consumer to Consumer
DES	Data Encryption Standard
d. h.	das heißt
Diss.	Dissertation
DIN	Deutsches Institut für Normung
DRM	Digital Rights Management
€	Euro
engl.	englisch
EBPP	Electronic Bill Presentment and Payment
EC	Eurocheque
ECB	European Central Bank
eds.	Editors (Herausgeber)
EDGE	Enhanced Data Rates for GSM Evolution

EG	Europäische Gemeinschaft
eGeld	Elektronisches Geld
EMS	Enhanced Messaging Service
EPS	Electronic Payment System(s)
ELV	Elektronisches Lastschriftverfahren im Zahlungsverkehr
et al.	(et alii, et aliae oder et alia) und andere
ETSI	European Telecommunications Standards Institute
EU	Europäische Union
EZB	Europäische Zentralbank
ff.	folgende
FTP	File Transfer Protocol
GG	Grundgesetz
GSM	Global System for Mobile Communications
GPRS	General Packet Radio Service
GPS	Global Positioning System
HBCI	Home Banking Computer Interface
Hrsg.	Herausgeber
HSCSD	High Speed Circuit Switched Data
HSPA	High Speed Packet Access
HTML	Hyper Text Markup Language
HTTP	Hypertext Transfer Protocol
IBM	International Business Machines Corporation
ID	Identifier/Identifikator
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
IP	Internet Protocol
IRC	Internet Relay Chat
ITU	International Telecommunication Union
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IrFM	Infrared Financial Messaging
IMEI	International Mobile Station Equipment Identity
IMPS	Instant Messaging and Presence Service
i. V. m.	in Verbindung mit
IVR	Interactive Voice Response

LAN	Local Area Network
LTE	Long Term Evolution
MAC	Media Access Control Adresse
MCP	Mobile Content Provider
Mio.	Million
MMA	Mobile Marketing Association
MMS	Multimedia Messaging Service
MNO	Mobile Network Operator
MPSP	Mobile Payment Service Provider
MTO	Money Transfer Operator
MDStV	Mediendienstestaatsvertrag
NFC	Near Field Communication
No.	Number
o. ä.	oder ähnliches
o. D.	ohne Datum
OHA	Open Handset Alliance
OMA	Open Mobile Alliance
OMTP	Open Mobile Terminal Platform
ÖPNV	Öffentlicher Personennahverkehr
o. V.	ohne Verfasser
PC	Personal Computer
P2P	Person to Person
P2P	Peer to Peer
PDA	Personal Digital Assistant
PIN	Personal Identification Number
POS	Point of Sale
POZ	Point of Sale ohne Zahlungsgarantie
Red.	Redaktion
RfStV	Rundfunkstaatsvertrag
RSA	Rivest, Shamir, Adleman (Erfinder von RSA-Verfahren)
RFID	Radio Frequency Identification
S.	Seite(n)

s.	siehe
SEMOPS	Secure Mobile Payment Service
SET	Secure Electronic Transaction
SIM	Subscriber Identity Module
SSL	Secure Socket Layer
SMS	Short Message Service
SOAP	Simple Object Access Protocol
sog.	so genannt
StPO	Strafprozessordnung
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TCP/IP	Transmission Control Protocol/Internet Protocol
TDG	Teledienstegesetz
TDDSG	Teledienstedatenschutzgesetz
TKG	Telekommunikationsgesetz
TKÜV	Telekommunikations-Überwachungsverordnung
TMG	Telemediengesetz
TOR	The Onion Router
TTP	Trusted Third Party
3GPP	Third Generation Partnership Project
3GPP2	Third Generation Partnership Project 2
UAE	United Arab Emirates (Vereinigte Arabischen Emirate)
UK	United Kingdom
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator
USA	United States of America
WAP	Wireless Application Protocol
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WML	Wireless Markup Language
W3C	World Wide Web Consortium
www	World Wide Web
XML	Extensible Markup Language
z. B.	zum Beispiel

IV. Abbildungsverzeichnis

Vorwort

Agieren in elektronischen Netzen, speziell dem Internet, fordert und bedarf eines gewissen Maßes an Vertrauen in die eingesetzten technischen, organisatorischen, prozessualen und rechtlichen Mechanismen und Regelungen der Informations- und Kommunikationsabwicklung. Die Vertrauenswürdigkeit dieser Regelungen muss für die Akteure hinlänglich einfach einsichtig und transparent sein. Die erfolgreiche Gestaltung dieser Vertrauensbeziehung kann sich also nicht auf die Implementierung prinzipiell sicherer und datenschutzrechtlich kompatibler Lösungen beschränken (notwendige Bedingung), sie muss auch Sorge tragen, dass diese Lösungen hinlänglich verstanden und also akzeptiert werden (hinreichende Bedingung). Erst die Implementierung dieser Vertrauensleistung in elektronische Prozesse sichert deren nachhaltigen Erfolg. Dies gilt für alle Internetaktivitäten, es gilt besonders für Kauf- und Zahlungstransaktionen, da hier Verletzungen der Vertrauenserwartungen i. d. R. auch materiellen Schaden zur Folge haben.

Ein Konzept zur Etablierung von Vertrauen in elektronische Prozesse bietet die Anonymisierung der persönlichen Daten der Prozessbeteiligten in einem allseits akzeptierten Umfang. Diese Einschränkung einer totalen Anonymisierung kann pragmatisch und/oder rechtlich motiviert sein. So kann die Schutznotwendigkeit vor Straftaten (z. B. Geldwäsche) dem Grad der praktizierten Anonymisierung Grenzen ziehen. Generell aber kann und sollte Anonymisierung die Persönlichkeits- und Informationsrechte der Prozessbeteiligten ausgewogen sichern. Dies aber impliziert zugleich, dass die Gestaltung der Anonymisierung multiperspektivisch ansetzen muss, also den unterschiedlichen Akteuren bzw. Rollen gerecht werden muss. Dieser Konflikt ist nur mittels Kompromiss lösbar. Die Rechtslage und –sprechung definiert dazu wichtige Rahmensetzungen, eröffnet für Technik und Organisation allerdings noch einen erheblichen Gestaltungsspielraum. Die Motivation, sich um allseits akzeptable Konzepte zu bemühen, resultiert aus dem Streben nachhaltig erfolgreiche Lösungen zu implementieren. Für den wachsenden Bereich der Geschäftstransaktionen vom mobilen Endgerät aus gelten alle traditionellen Internet-Business-Probleme ebenso.

Hinzu kommen spezielle Informationen über die Ortskoordinaten des Teilnehmers. Auch die Gefahren des Missbrauchs steigen bei Verlust oder Diebstahl des Endgeräts. Beiden Gefahren kann durch Anonymisierung bedingt begegnet werden.

Dem gesamten Komplex des mobilen Zahlungsverkehrs widmet sich die Dissertation „User-Anonymität in Mobile Payment Systemen. Ein Referenzprozessmodell zur Gestaltung der User-Anonymität in Mobile Payment Systemen“ von Herrn Feyyat Kaymaz. Und dies umfasst Zahlungen vom mobilen Endgerät im Rahmen eines klassischen Internetgeschäftsvorgangs, aber auch die Bezahlung von Leistungen am POS (Supermarktkasse, Parkautomat, ÖPNV-Automaten etc.). Die auf dem Markt angebotenen Lösungen werden sorgfältig untersucht und auf ihre Brauchbarkeit zur Herstellung „steuerbarer“ Anonymität bewertet. Ein („ideales“) Referenzmodell zur „anonymen Zahlung“ wird als innovatives Ergebnis vorgelegt. Hervorzuheben ist das weithin gelungene Bemühen der komplexen Thematik durch Einbindung multidisziplinären Wissens in den Lösungsansatz gerecht zu werden. Die ökonomischen, technischen, juristischen, organisations- und verhaltenstheoretischen Facetten der Thematik werden in dem Konzept des Referenzmodells zusammengeführt. Die Arbeit leistet einen gewichtigen konzeptionellen Beitrag zur Umsetzung von Anonymisierungsverfahren.

Köln, den 12. August 2011

Prof. Dr. Udo Winand

Danksagung

Ungeachtet der Tatsache, dass die Erarbeitung einer Dissertation ein hohes Maß an persönlichem Einsatz, Ausdauer und Verzicht erfordert, möchte ich gerne vielen Menschen mein herzliches Dankeschön aussprechen, die mich während meiner Promotion begleitet und unterstützt haben. Sie brachten mir sehr viel Geduld entgegen und sorgten mit wertvollen Ratschlägen für das Gelingen der Dissertation.

An erster Stelle bedanke ich mich bei meinem Doktorvater, Herrn Prof. Dr. Udo Winand, der die wissenschaftliche Betreuung meiner Dissertation übernommen und mich durch methodische Anregungen und kritische Fachdiskussionen unterstützt hat. Ich bedanke mich ebenfalls bei Herrn Prof. Dr. Gerd-Michael Hellstern für die Übernahme des Zweitgutachtens.

Mein großer Dank gilt auch allen Korrekturlesern und Kommentatoren, insbesondere Jutta Heinen, Dr. Alexander Balke, Michael Möglich und RA Sandra Engels, die mit ihrem breiten Wissen viele Anregungen für meine wissenschaftliche Arbeit gegeben und somit zur Fertigstellung dieser Arbeit einen wichtigen Beitrag geleistet haben.

Schließlich bedanke ich mich bei den Mitgliedern der Prüfungskommission, Prof. Dr. Udo Winand, Prof. Dr. Gerd-Michael Hellstern, Prof. Dr. Alexander Roßnagel und Prof. Dr. Rainer Stöttner für die Durchführung meiner Disputation.

Ich widme diese Dissertation meiner großartigen Familie.

Düsseldorf, den 29. August 2011

Feyyat Kaymaz

1 Einführung

1.1 Motivation und Problemstellung

Die technologischen Entwicklungen in mobilen Telekommunikationsgeräten eröffnen neue Kommunikationswege und Geschäftsfelder. Die Mobilfunkgeräte wie Handy, PDA und Smartphone etc. sind zu wichtigen Kommunikationsinstrumenten in der Gesellschaft geworden und werden fast überall eingesetzt.[1] Diese Mobilfunkgeräte ersetzen den heimischen PC und ermöglichen einen zeit- und ortunabhängigen Zugang zum Internet. Der mobile User[2] ist überall und fast immer online und somit erreichbar. Er kann mit seinem Mobilfunkgerät einkaufen oder einen Service anfordern und diesen mobil bezahlen. Mobile Payment ermöglicht im Mobile Commerce die Bezahlung der Produkte und Services.[3] Auch wenn die Nutzung der Mobile Payment zurzeit noch nicht verbreitet ist, wird jedoch erwartet, dass sich dies in den kommenden Jahren schnell ändern und die Nutzung von Mobile Payments zunehmen wird.

Die Mobilität der User sowie die mobilen Geschäftsprozesse werden immer komplexer. In einer vernetzten und komplexen Digitalwelt werden immer mehr Daten und Informationen ausgetauscht. Diese Entwicklung wirft neue Fragen zur Sicherheit, Privatsphäre und Anonymität der Nutzung mobiler Services auf. Bei jeder Transaktion hinterlassen mobile User bewusst oder unbewusst eine große Menge von Datenspuren. Bei den Transaktionen werden sehr viele allgemeine, persönliche und

---

1 Die Begriffe Handy, Smartphone und ähnliche Endusergeräte werden zusammengefasst und innerhalb dieser Dissertation einheitlich als Mobilfunkgerät bzw. Mobilfunkgeräte bezeichnet. Unter dem Begriff Handy wird ein Mobiltelefon, also ein tragbares Telefon verstanden, das über Funknetze funktioniert und ortunabhängig benutzt werden kann. Der Begriff PDA (Personal Digital Assistant) bezeichnet ein kleineren, tragbaren Minicomputer, der vor allem für die Verwaltung von Adressen, Aufgaben und Kalender eingesetzt wird. Gegenwärtig werden diese PDAs durch Smartphones ersetzt. Smartphones sind die Mobiltelefone mit den PDA-Eigenschaften. Sie haben eigenes Betriebssystem und viele verschiedene Internet- und Office-Anwendungen etc. Vgl. Logara (2007), S. 73ff.

2 Der englische Begriff User wird innerhalb dieser Arbeit je nach dem Kontext synonym für die Begriffe Kunden, Konsumenten, Nutzer und Benutzer verwendet. Dabei wird unter dem Begriff User eine Person, die etwas kauft und verwendet, verstanden. Im Zusammenhang mit der Mobilität der User wird der Begriff der mobile User verwendet.

3 Die Begriffe Mobile Commerce und Mobile Payment sind im internationalen Umfeld entstanden und sowohl im geschäftlichen als auch akademischen Bereich akzeptiert und gebraucht. Deshalb werden diese Begriffe in dieser Dissertation in englischer Sprache verwendet.

vertrauliche Informationen an die Marktteilnehmer insbesondere die Händler[4] übertragen. Schon bei einer Bestellung oder Servicenutzung teilt der mobile User seine personenbezogenen Daten dem Händler mit. Was die Händler mit diesen personenbezogenen bzw. sensiblen Daten der User machen, ist vielen Usern gar nicht oder selten bekannt und wird von diesen kaum wahrgenommen. Die sensiblen Daten und Informationen können ohne Kenntnis der User zu legalen oder illegalen Zwecken verwendet, weitergegeben oder weiterverkauft werden. Durch die hinterlassenen bzw. übertragenen Daten können individuelle und kollektive Persönlichkeitsprofile erstellt werden. Diese Daten und Informationen verschaffen Potenziale für Betrug, Manipulation und Missbrauch. Diese Potentiale können sowohl von staatlichen Finanz- oder Sicherheitsbehörden, als auch von der privaten Wirtschaft und von kriminellen Personen(-gruppen) gebraucht werden.[5] Händler, Kreditinstitute, Telekommunikationsunternehmen und Staat können Persönlichkeitsprofile hinsichtlich des Kaufverhaltens oder Verhaltensmuster anhand des Aufenthaltsorts etc. von Kunden[6] oder Bürgern erstellen.[7]

In diesem Zusammenhang gewinnen die Begriffe Schutz der Privatsphäre, Datenschutz und informationelle Selbstbestimmung immer mehr an Bedeutung. Aus diesen Gründen ist die Anonymität der User eine sehr wichtige Sicherheitsanforderung und ein sehr wichtiges Persönlichkeitsrecht. Beispielsweise möchte ein mobiler User beim Kauf bzw. Bezahlung der erwachsenenspezifischen Produkte und Services die eigene Identität nicht preisgeben, um seine Privatsphäre zu schützen. Um den Usern eine gewisse Anonymität ermöglichen zu können, müssen neue Schutzvorkehrungen getroffen werden. Dies erfordert die Gestaltung neuartiger Maßnahmen und Regeln in den Mobile Payment Systemen. Da die Anonymität neben den Vorteilen auch einige Nachteile mitbringt, soll auch die Gesellschaft auf der anderen Seite die Möglichkeit haben, gegen die Nachteile der Anonymität vorzugehen, die durch die Gewährleistung der User-Anonymität hervorgerufen werden könnten.

---

4 Der Begriff Händler wird innerhalb dieser Arbeit je nach Kontext synonym für die Begriffe Anbieter, Verkäufer sowie Provider verwendet. Dabei wird unter dem Begriff Händler jemand verstanden, der eine Dienstleistung vollbringt.

5 Vgl. ULD (2002), S. 4ff.

6 Kunde bedeutet hier im weitesten Sinne sowohl Endkunde als auch den Händler als Kunden von Telekomunternehmen und Banken, denn auch diese können Informationen über ihre Kunden besitzen, wie z. B. Geschäftszahlen und Kundenprofile etc.

7 Vgl. ULD (2002), S. 4ff.

Aus der dargestellten Problematik stellen sich folgende Fragen, die es in dieser Dissertation zu erörtern und beantworten gilt:

- Was ist Mobile Payment?
- Welche Marktteilnehmer gibt es? Welche Interessen verfolgen und welche Anforderungen stellen die einzelnen Marktteilnehmer?
- Was ist Anonymität? Was sind deren Vor- und Nachteile?
- Wann und Warum wird die User-Anonymität in Mobile Payment Systemen benötigt?
- Was ist der Zusammenhang zwischen Anonymität und Sicherheit?
- Wie können sichere und anonyme Zahlungen abgewickelt werden?
- Wie kann die User-Anonymität hergestellt werden?
- Unter welchen Bedingungen kann die User-Anonymität hergestellt werden?
- Welche Möglichkeiten existieren für die Herstellung der User-Anonymität in M-Payment Systemen?
- Welche organisatorischen, technischen und rechtlichen Rahmenbedingungen werden für die Gestaltung der User-Anonymität Mobile Payment Systemen benötigt?
- Welche Gestaltungsmöglichkeiten für die User-Anonymität existieren? Was ist dabei zu berücksichtigen?
- Welche Probleme und Risiken tauchen auf? Welche Lösungsmöglichkeiten existieren?

1.2 Zielsetzung und Lösungsansatz

Das Hauptziel dieser wissenschaftlichen Auseinandersetzung besteht in der Gewinnung neuer Erkenntnisse über die Lösung der geschilderten Problematik, mithin die Entwicklung eines organisatorischen Konzepts für die Gestaltung der User-Anonymität in Mobile Payment Systemen. Dabei werden die Möglichkeiten für den Schutz der eigenen Identität und Privatsphäre vor Manipulation und Missbrauch untersucht.

Hierfür wird zunächst die Problematik und Bedeutung der User-Anonymität in Mobile Payment Systemen dargestellt. Für die Aufstellung eines solchen Konzeptes werden

die organisatorischen, technischen und rechtlichen Rahmenbedingungen zur Gestaltung der User-Anonymität in Mobile Payment Systemen untersucht werden. Um die User-Anonymität gewährleisten zu können, müssen vorhandene Anonymitätskonzepte genutzt oder neue Konzepte, Richtlinien und Gesetze entwickelt werden. Nach den gewonnenen Erkenntnissen wird ein Ansatz zur Lösung der Problematik präsentiert und ein organisatorisches Konzept aufgestellt, mit dem die Anonymität der User in Mobile Payment Systemen gewährleistet werden kann, wobei die Interessen anderer Marktteilnehmer berücksichtigt werden.

Damit das Konzept seine Ziele erreichen kann, müssen einige wichtige Anforderungen in Betracht gezogen werden:

1. Bei mobilen Zahlungstransaktionen sollen die persönlichen Daten und Informationen vertraulich behandelt werden.

2. Der Umgang mit den vertraulichen Daten und Informationen soll durch den Einsatz und die Nutzung von neuen Techniken, Verfahren, Richtlinien und Gesetze gewährleistet werden.

3. Die legalen Interessen von Marktteilnehmern sollen bei Mobile Payment Transaktionen berücksichtigt werden.

4. Die mobilen Zahlungstransaktionen sollen, wenn die Marktteilnehmer, vor allem die mobilen User, dies wünschen, genauso wie Bargeldzahlungen anonym abgewickelt werden. Die User können nicht zuletzt wegen der informationellen Selbstbestimmung in der Lage sein, ihre Anonymität zu erkennen und gegebenenfalls zu kontrollieren.

5. Um den Usern eine bestimmte Anonymität ermöglichen zu können, werden verschiedene Möglichkeiten angeboten. Unter anderem können sie ihre Identität durch verschiedene Anonymisierungsdienste im beschränkten bis vollem Umfang bewahren.

Die Ziele dieser Dissertation lassen sich wie folgt formulieren:

- Würdigung der Bedeutung der User-Anonymität in Mobile Payment Systemen
- Erstellung eines Überblicks über die Mobile Payments, die Marktteilnehmer und deren Interessen und Anforderungen

- Entwicklung und Anwendung neuer Paradigmen: Die Überprüfung der Möglichkeiten zur Herstellung und Bewahrung der User-Anonymität sowie die Untersuchung der Gestaltungsmöglichkeiten zur Vermeidung der Beobachtung des Userverhaltens und Verkettung der Daten und Informationen. Die User sollen die Möglichkeit haben, ihre Anonymität in Mobile Payment Systemen zu steuern bzw. zu kontrollieren.

- Optimale Verknüpfung verschiedener Lösungsansätze: Im Rahmen dieser Dissertation werden die am Markt befindlichen Möglichkeiten zur Zahlung dargestellt, ihre Anonymität untersucht und ein ideales Modell zur anonymen Zahlung vorgestellt.

- Suche nach effektiven und effizienten Werkzeugen und Technologien: Welche organisatorischen, technischen und regulatorischen Maßnahmen sollen getroffen werden, um einen bestimmten Grad der Anonymität bei Mobile Payment Systemen herzustellen?

Für die Verfolgung des Forschungsgegenstandes wird die folgende These zugrunde gelegt: Die Anonymität ist dann bedeutsam und gefordert, wenn die oben geschilderten Sicherheits- und Anonymitätsbedenken in Mobile Payment Systemen bestehen. Wenn die entsprechenden Kriterien erfüllt werden können, dann kann die User-Anonymität in Mobile Payment Systemen gewährleistet werden. Hierfür sollen die Anforderungen von Marktteilnehmern bestimmt und ein Kriterienkatalog entwickelt werden. Durch diese Kriterien können dann neue Verfahren bzw. Konzepte zur Bewahrung der User-Anonymität in Mobile Payment Systemen entworfen werden.

Diese neuen Konzepte sollen Anonymisierungsdienste schaffen bzw. einen Beitrag dazu leisten, um anonyme Zahlungstransaktionen im M-Commerce gewährleisten zu können. Hierfür soll die Übertragbarkeit von existierenden Lösungen und Verfahren zur User-Anonymität sowie zur Anonymisierung im Internet dahingehend überprüft werden, inwiefern diese auch für das Mobile Payment eingesetzt werden können.

Die Innovation dieser Dissertation besteht in der Übertragbarkeit von existierenden Lösungen bzw. Verfahren zu einem neuartigen Lösungsansatz und der Machbarkeit eines solchen Lösungsansatzes zur User-Anonymität in Mobile Payment Systemen. Der Schwerpunkt liegt dabei in der Entwicklung eines neuen organisatorischen Konzeptes, das die User-Anonymität in Mobile Payment Systemen gewährleisten soll. Dieses organisatorische Konzept wird anhand eines Beispiels in einem Referenz-

prozessmodell erklärt. Des Weiteren werden Anforderungen und Rahmenbedingungen für die Gestaltung der User-Anonymität bestimmt sowie Realisierungswege eines derartigen Lösungsansatzes für die Marktteilnehmer gezeigt.

1.3 Forschungsstand

Das Thema Mobile Payment ist einer der meist untersuchten Themenbereiche im M-Commerce. Dies kann anhand der bisher veröffentlichten Artikel und wissenschaftlichen Arbeiten über Mobile Payments schlussgefolgert werden. Die meisten in der Literatur befindlichen Quellen liefern eine Momentaufnahme und Klassifizierung von derzeitigen Mobile Payment Systemen. Dabei wurden bisher viele technikorientierte Forschungsarbeiten geleistet. Diese konzentrieren sich größtenteils auf die Machbarkeit und Sicherheit, also auf die technischen und kryptografischen Seiten von Mobile Payments. Außerdem wurde das Thema Anonymität in Verbindung mit Internet oder Mobilität aus der Perspektive der Informatik behandelt, indem sich die Arbeiten auf die technische Realisierbarkeit konzentrierten.[8]

Das Thema Anonymität wurde zudem auch aus rechtlicher Perspektive schon behandelt. So gibt es auch Untersuchungen zur rechtlichen Gestaltung von Mobile Payments, in der die Anonymität und Pseudonymität aus rechtlicher Sicht behandelt wurden.[9] Darüber hinaus wurden einige Forschungsarbeiten in den verhaltensorientierten Untersuchungen im Bereich Mobile Payments geführt. So hat man z.B. Akzeptanzmöglichkeiten von Mobile Payments untersucht.[10] Gleichzeitig wurden die Anforderungen von User und anderen Marktteilnehmer an Mobile Payments erforscht.[11]

In letzter Zeit orientiert sich die Forschung im Lichte der verhaltensorientierten Forschungsergebnisse in die Richtung der gestaltungsorientierten Erforschung[12] von Mobile Payments. Unter anderem werfen das Zusammenwachsen von mobilen Technologien und Anwendungen sowie Marktentwicklungen viele Fragestellungen auf, die neue Forschungsarbeiten erforderlich machen. Diese Orientierung befindet

---

8 Vgl. Federrath/Martius (1998); Federrath (2003); Pfitzmann/Hansen (2009); Hansen/Meissner (2007).

9 Vgl. Stadler (2006).

10 Vgl. Pousttchi/Selk/Turowski (2002).

11 Vgl. Henkel (2001); Henkel (2002).

12 Vgl. Becker/Krcmar/Niehaves (2009).

sich derzeit in den Anfängen. Bisherige gestaltungsorientierte Forschungsarbeiten wurden unter anderem in der Bildung eines Referenzmodells für alle Mobile Payment Vorgänge durchgeführt.[13] Außerdem wurde das Thema „Anonymität“ im Bereich Mobile Payment aus der Perspektive der Wirtschaftsinformatik bisher nicht ausreichend untersucht. Daher gibt es bisher wenige gestaltungsorientierte Untersuchungen im Bereich Mobile Payments.

Mit dieser Dissertation wird ein innovativer Beitrag zur Lösung der Problematik der User-Anonymität in Mobile Payment Systemen geleistet. Mit diesen Erkenntnissen wird die Wissenslücke in den Forschungsbereichen User-Anonymität und Mobile Payment geschlossen. Die Erforschung der Thematik der User-Anonymität in Mobile Payment Systemen soll aus der Perspektive der Wirtschaftsinformatik erfolgen und neue Erkenntnisse für die Weiterentwicklung von Mobile Payment Systemen gewinnen, mit deren Hilfe die dargestellten Problematiken gelöst werden können.

1.4 Methodik

Bei der Durchführung der Forschung wurden die Methoden der konzeptionell-deduktiven Analyse und der Referenzmodellierung genutzt. Diese Methodik ist ein konstruktionsorientierter Ansatz der Wirtschaftsinformatik, mit dessen Hilfe eine konzeptionelle Lösung entworfen werden kann.[14] Für den Entwurf einer organisatorischen Konzeptlösung ist eine sequentielle Vorgehensweise zweckmäßig, die in der Abbildung 1, S. 11 dargestellt wird. Diese Vorgehensweise wird im Folgenden detailliert beschrieben.

Im ersten Kapitel wird in die Thematik Mobile Payment und Anonymität des Users eingeführt. Hierfür wird zuerst die Motivation für die Forschung und Problemstellung in den Bereichen Mobile Payment und User-Anonymität dargestellt. Danach werden die Ziele dieser Forschung definiert, um einen Lösungsansatz für die Problematik zu finden. Im nächsten Abschnitt wird ein Überblick über die bisherigen Forschungsarbeiten gegeben, damit die Forschung in dieser Dissertation innerhalb des relevanten Forschungsbereiches eingeordnet werden kann. Im letzten Abschnitt wird die Forschungsmethodik und Vorgehensweise dargestellt.

---

[13] Vgl. Pousttchi (2003); Pousttchi (2005).

[14] Vgl. Wilde/Hess (2006), S. 4ff.

Im zweiten Kapitel werden die Grundlagen von Mobile Payments dargelegt, welche für dessen grundlegendes Verständnis erforderlich sind. Für diesen Zweck wurde eine Quellenanalyse der jeweiligen Literatur und der Praxis durchgeführt. Zunächst wird ein kurzer Überblick über die Innovationen und Trends im Bereich „Mobile“ gegeben, die für Mobile Payment relevant sind. Danach wird eine begriffliche Einordnung und Definition von Mobile Payment erläutert sowie der Stellenwert von Mobile Payment im M-Commerce betont. Im nächsten Abschnitt werden die Typen von Mobile Payment im M-Commerce differenziert und im Rahmen einer Klassifikation dargestellt. Darauf folgen ein Überblick über die eingesetzten Technologien sowie ein Überblick über die Anwendungsbereiche von Mobile Payment Systemen. Außerdem werden die Mobile Payment-Initiativen erläutert.

Im dritten Kapitel wird eine Analyse des Mobile Payment Ökosystems[15] durchgeführt. Hierfür wird erläutert, welche Marktteilnehmer im Ökosystem von Mobile Payment auftreten und worin deren Rollen und Beziehungen zueinander bestehen. Danach wurden die Interessen und Anforderungen von Marktteilnehmern analysiert. Dabei werden die Probleme und Konflikte einzelner Marktteilnehmer, insb. der User und Händler, nach ihrer Art und Relevanz gezeigt. Zu diesem Zweck wurde ebenfalls eine Quellenanalyse der jeweiligen Literatur und Praxis durchgeführt.

Im vierten Kapitel werden die Grundlagen der Anonymität geschaffen. Hierfür wurde eine Quellenanalyse der jeweiligen Literatur und der Praxis durchgeführt. Zunächst wird ein kurzer Überblick über die Schutzziele der Informations- und Kommunikationssicherheit gegeben. Danach wird die Anonymität als ein Schutzziel der Informationssicherheit erläutert sowie der Begriff „Anonymität“ definiert. Im nächsten Anschnitt wird eine Übersicht über die Formen der Anonymität geschaffen. Zudem wird der Begriff „Identität“ sowie Grade der Anonymität erläutert. Darauffolgend wird die Anonymität im Internet und mobilen Kommunikationsnetzwerken erläutert. Außerdem werden die Argumente pro und contra Anonymität vorgestellt.

Im fünften Kapitel werden die Rahmenbedingungen für die Gestaltung der User-Anonymität dargestellt. Hierfür wurden die organisatorischen, technischen und regu-

[15] Der Begriff „Ökosystem“ wird als ein System definiert, dessen Mitglieder von der jeweils anderen Teilnahme über symbiotischen Beziehungen profitieren. Der Begriff stammt von der Biologie und bezieht sich auf selbstversorgende Systeme. Vgl. http://www.answers.com/topic/ecosystems-1, Stand: 28.01.2010. Der Begriff „Ökosystem“ im Sinne des Wirtschaftslebens wird als ein System definiert, in dem die Beziehungen verschiedener Personen, Organisationen und Industrien auf gegenseitige Vorteile basieren. Vgl. http://www.definethat.com/define/302.htm, Stand: 28.01.2010.

latorischen Rahmenbedingungen für die Gestaltung der User-Anonymität erläutert. Hierzu wurde ebenfalls eine Quellenanalyse der jeweiligen Literatur und der Praxis durchgeführt. In den organisatorischen Rahmenbedingungen wird die Definition und Organisation der Daten und Informationen aus der Perspektive des Datenschutzes erklärt. In den technischen Rahmenbedingungen werden neben den anonymen Server-Systemen und Netzwerken die Anonymitätskonzepte und deren Praxisbeispiele dargestellt. In regulatorischen Rahmenbedingungen werden die Richtlinien und Gesetze sowie strafrechtlichen Aspekte der Anonymität erklärt.

Im sechsten Kapitel wird auf die Thematik der Anonymität in Mobile Payment Systemen eingegangen. Hierzu wird eine Quellenanalyse der jeweiligen Literatur und der Praxis durchgeführt. Anschließend werden die Ergebnisse dieser Analysen mit den Analyseergebnissen des zweiten bis vierten Kapitels zusammengeführt. Zunächst wird die Bedeutung der User-Anonymität in Mobile Payment Systemen aus soziologischer und ökonomischer Sicht erklärt. Dann werden die Mobile Payment Wertschöpfungskette sowie ein allgemeiner Mobile Payment Prozess beschrieben. Anschließend wird der allgemeine Mobile Payment Prozess hinsichtlich der User-Anonymität bewertet. Damit werden die Schwachstellen der Phasen dieses Prozesses gezeigt, in denen die Anonymisierung bzw. Pseudonymisierung erfolgen sollten. Im nächsten Schritt wird ein neues Referenzprozessmodell für die Gestaltung der User-Anonymität in Mobile Payment Systemen dargestellt. Dies wurde auf der Basis der gewonnenen Analyseergebnisse des zweiten bis fünften Kapitels entworfen. Hierfür wird der Mobile Payment Prozess mit den einzelnen Phasen beschrieben, indem die User-Anonymität gewährleistet werden kann. Danach wird die User-Anonymität gegenüber den einzelnen Marktteilnehmern im Referenzprozessmodell bewertet.

Im siebten Kapitel werden die Wege zur Realisierung des Referenzprozessmodells und Gestaltungsmöglichkeiten der User-Anonymität in Mobile Payment Systemen gezeigt. Zu diesem Zweck werden die Analyseergebnisse des fünften und sechsten Kapitels zusammengeführt. Hierfür wird auf die Handlungsmöglichkeiten hingewiesen und Handlungsempfehlungen für die Betroffenen gegeben. Für die Bewertung der Gestaltungsmöglichkeiten werden drei Analysen geführt. Im ersten Schritt wird die Berücksichtigung und Erfüllung der Anforderungen im Referenzprozessmodell analysiert. Im zweiten Schritt wird die Berücksichtigung und Erfüllung der Rahmenbedingungen im Referenzprozessmodell analysiert, wobei die organisatorischen, technischen und regulatorischen Gestaltungsmöglichkeiten gezeigt werden. Der Fokus liegt dabei in der Analyse und Bewertung der organisatorischen

Gestaltungsmöglichkeiten. Im dritten Schritt werden die potentiellen Risiken und Probleme bei der Gestaltung der User-Anonymität gezeigt.

Im achten Kapitel erfolgt ein Fazit. Hierfür werden zunächst die Ergebnisse der Forschung zusammengefasst. Daraus werden dann die Schlussfolgerungen abgeleitet. Anschließend wird auf die offenen Fragen verwiesen und ein Ausblick auf die zukünftigen Entwicklungen und möglichen Forschungsfragen in den Bereichen Anonymität und Identitätsmanagement in Mobile Payment gegeben.

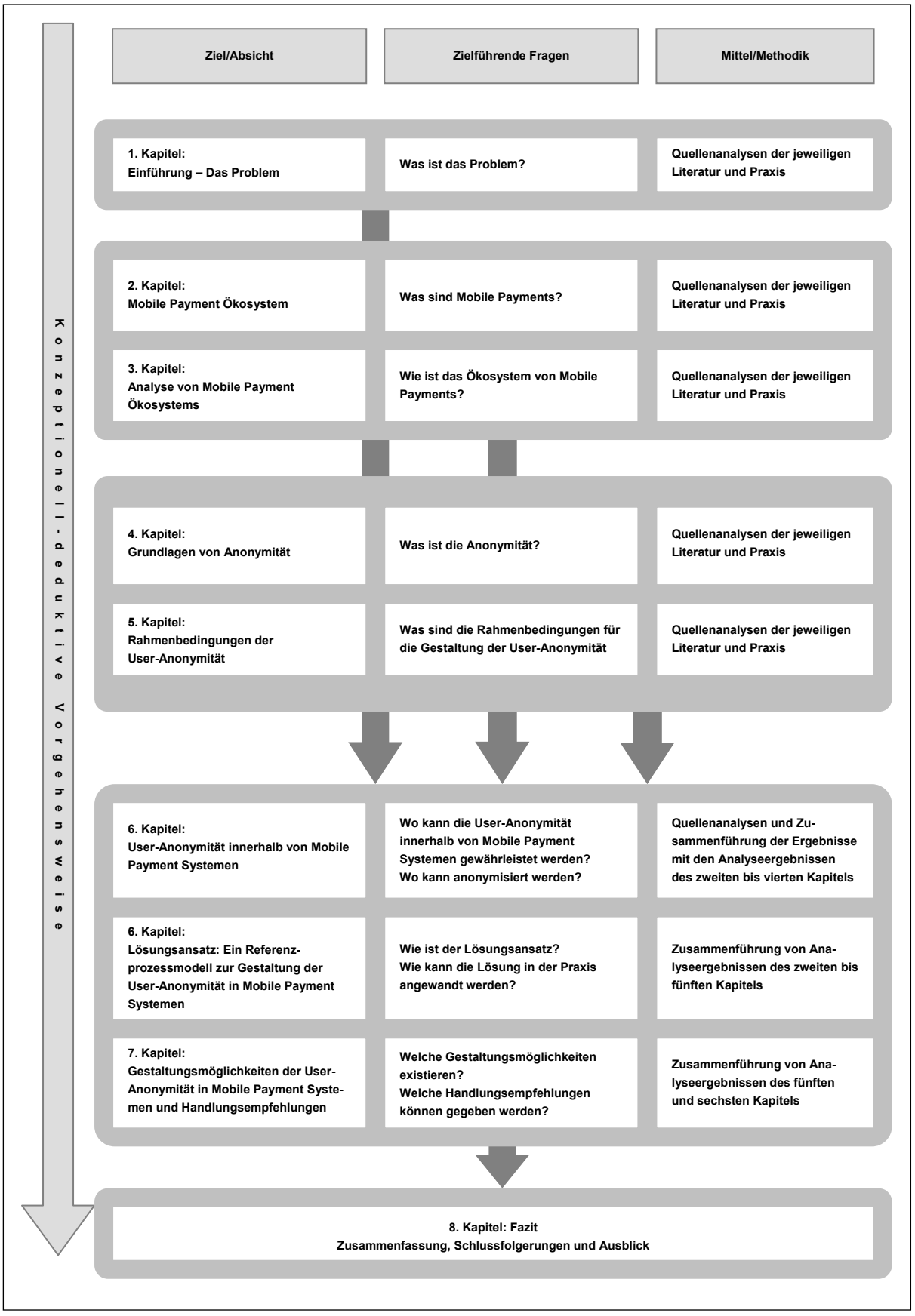

Abbildung 1: Schematische Darstellung der Forschungsmethodik

2 Mobile Payment Ökosystem

Zum besseren Verständnis der Thematik soll das Mobile Payment Ökosystem erklärt werden. Zu diesem Zweck werden zunächst die Innovationen und Trends im Bereich Mobile Commerce und Mobile Payment erläutert. Danach wird der Begriff Mobile Payment definiert und im Kontext der Electronic und Mobile Business-Prozessen und -Technologien eingeordnet. Es wird auch erläutert, welche Rolle Mobile Payment im Mobile Commerce spielt bzw. welchen Stellenwert Mobile Payment hat. Dann wird erklärt, welche Mobile Payment Typen existieren. Im nächsten Abschnitt erfolgt eine Klassifikation von Mobile Payment Systemen, um zu zeigen, welche Infrastrukturen und Systeme hinter Mobile Payments stehen. Dabei werden ein Überblick über die Technologien, die für die Mobile Payment Systeme verwendet werden, sowie ein Überblick über die Anwendungsbereiche von Mobile Payment gegeben. Für die Entwicklung und Durchsetzung von Technologien bzw. Standards, die bei der Gestaltung der User-Anonymität entscheidende Rolle spielen, gibt es einige Initiativen und Kooperationen zwischen den Marktteilnehmern im Mobile Payment, die es ebenfalls zu erläutern gilt. Deshalb wird auch erklärt, welche Initiativen und Kooperationen im Bereich Mobile Payment bestehen.

2.1 Innovationen und Trends im Bereich „Mobile“

Gegenwärtig sind im Bereich „Mobile“ insb. im Mobile Commerce und Mobile Payment rasante Entwicklungen zu beobachten. Die Mobilfunkgeräte wie Handy oder Smartphone werden mit immer mehr Funktionalität ausgestattet. Die mobilen User nutzen ihre Mobilfunkgeräte nicht nur für die Kommunikation, sondern auch für den Einkauf und die Bezahlung unterwegs. Es dürfte sehr wahrscheinlich sein, dass die Nachfrage nach den Einkaufs- und Bezahlungsmöglichkeiten mit den Mobilfunkgeräten bedeutsam steigen wird. Gleichzeitig wird auch die Gestaltung der mobilen Einkaufs- und Bezahlungsmöglichkeiten zunehmen. Insbesondere werden die Einkäufe alltäglicher Güter, Essen und Getränke sowie Haushaltsware über die Mobilfunkgeräte getätigt werden. Die mobilen User werden viele Einkaufs- und Zahlungstransaktionen unabhängig vom Standort und der Tageszeit durchführen können. Die Anbieter der Webshops und mobiler Services können diese Chance nutzen, entsprechende mobile Einkaufs- und Bezahlungsmöglichkeiten zu gestalten. Die Innovationen und Trends im Bereich „Mobile“ gehen besonders in die Richtung

folgender Bereiche, die von Gartner Research als die Top 10 Mobile Anwendungen für 2012 identifiziert wurden:[16]

1. Money Transfer[17]
2. Location Based Services[18]
3. Mobile Search: Mobile Suchmaschinen wie z. B. Google mobile, Yahoo! mobile sollen neue mobile Marketing und Vertriebsmöglichkeiten auf den Mobilfunkgeräten eröffnen.
4. Mobile Browsing: Optimierte Mobile Browser für mobile Web-Content, z. B. Opera mini, Safari, Windows phone.
5. Mobile Health Monitoring: Mobile Gesundheitsüberwachung der Patienten durch den Einsatz der IT und mobiler Endgeräte, z. B. Cencurio.
6. Mobile Payment[19]
7. Near Field Communication (NFC) Services[20]
8. Mobile Advertising: Das ist eine Form der Werbung über die Mobilfunkgeräte und Teilmenge des Mobile Marketings, z. B. T-Mobile.
9. Mobile Instant Messaging: Darunter wird das Chatten über die Mobilfunkgeräte verstanden. Beispiele sind MSN, Yahoo!, Google Talk, ICQ und Twitter etc.
10. Mobile Music: Darunter wird die Musik verstanden, die von mobilen Usern heruntergeladen oder per Streaming an die Mobilfunkgeräte gesendet und von dort gespielt werden kann, z. B. T-Mobile Music.

Neben diesen genannten Trends und Innovationen können auch die folgenden Trends erwähnt werden, die im Zusammenhang mit dem Thema Mobile Payment stehen:

- Contactless Payments
- Mobile Marketing

---

16 Vgl. Gartner (2009b).

17 Dies wird im Abschnitt 2.1.1 Mobile Money Transfer, S. 14 näher erläutert.

18 Dies wird im Abschnitt 2.1.2 Location Based Services, S. 14 ausführlich behandelt.

19 Dies wird im Abschnitt 2.1.3 Mobile Payment, S. 15 näher erklärt.

20 Dies wird im Abschnitt 2.1.4 Near Field Communication Services, S. 16 detailliert erläutert.

- Mobile Social Networking

Im Folgenden werden die Innovationen und Trends aufgrund der Relevanz und des Zusammenhangs mit dem Thema Mobile Payment erläutert.

2.1.1 Mobile Money Transfer

Mobile Money Transfer ermöglicht es, mobilen Usern Geld per SMS, USSD etc. an andere zu senden bzw. zu empfangen. Dieser mobilen Anwendung wird eine große Aufmerksamkeit geschenkt, da dies aufgrund der Einfachheit, niedrigeren Kosten und schnelleren Geschwindigkeit im Vergleich zu traditionellen Geldtransfermöglichkeiten einen größeren Erfolg verspricht. Money Transfer ist eng mit Mobile Remittance verbunden und hat in den Entwicklungsländern (insb. in Afrika und Asien) innerhalb des ersten Jahres Millionen von Usern verzeichnet, z. B. M-Pesa, Obopay und SMART.[21] Jedoch stehen die Marktteilnehmer vor neuen Herausforderungen in organisatorischen, ordnungsrechtlichen sowie technischen Risiken und Gefahren. Aufgrund des schnellen Wachstums von Mobile Money Transfer müssen die Regulierungsbehörden in diesen Ländern die Auswirkungen der Kosten, der Sicherheit, des Betrugs und der Geldwäsche untersuchen. Auf der operativen Seite variieren Marktbedingungen bzw. die lokalen Ressourcen. Deshalb brauchen Service Provider unterschiedliche Strategien, wenn sie beabsichtigen in diesen Ländern zu operieren.[22]

2.1.2 Location Based Services

Die Location Based Services (LBS) sind mobile standortbezogene Dienste, die mit Hilfe von Standort- und Zeitdaten sowie personenbezogenen Daten selektive Informationen und andere Dienste dem mobilen User zur Verfügung stellen. Die Produktinformationen und der Verkauf werden dem mobilen User basierend auf LBS und Near Field Communication (NFC) möglich gemacht.[23] Beispiele sind die Einkaufsmöglichkeiten, Preisinformationen für landwirtschaftliche Erzeugnisse an nahegelegenen Marktplätzen, Sehenswürdigkeiten in der Nähe des Standortes, Stadt- und Routenplan etc. Mit den LBS werden die mobilen User z. B. über die Produkte

---

[21] Vgl. Ebenda und Agrawal (2009) sowie die Erläuterungen im Abschnitt 2.7.4 Mobile Remittance, S. 46.

[22] Vgl. Gartner (2009b).

[23] Vgl. mit dem Abschnitt 2.6.2.1 Near Field Communication, S. 36 sowie mit dem Abschnitt 2.1.4 Near Field Communication Services, S. 16.

und Sonderangebote in den Geschäften in der räumlichen Nähe des Users informiert. So können die mobilen User die mobilen Netzwerke, in der sie sich gerade befinden, auswählen, die den Usern SMS-Nachrichten über Geschäfte und deren Produkte und Angebote senden, die für den aktuellen Standort der mobilen User interessant sind. Laut Gartner wird die Anzahl der LBS-User weltweit von 96 Mio. im Jahr 2009 auf mehr als 526 Mio. im 2012 wachsen.[24] Bei der Nutzung der LBS besteht allerdings das Risiko, dass die Anbieter der LBS personenbezogene Daten zusammen mit Standort- und Zeitdaten an Dritte weitergeben können. Auf diese Weise können diese Daten und Informationen miteinander verkettet werden, was die User-Anonymität beeinträchtigt.[25]

2.1.3 Mobile Payment

Mobile Payment wird als eine mobile Zahlungstransaktion, die durch mobile Endgeräten initiiert werden, bezeichnet und ist eine sehr wichtige Applikation für Mobile Commerce.[26] Mobile Payment erfüllt in der Regel drei Zwecke:[27] Erstens ist es eine weitere Möglichkeit zur Zahlung, wenn gerade nur wenige oder keine Alternative verfügbar ist. Zweitens ist es eine Erweiterung der Online-Payment-Möglichkeiten aufgrund mobiler Verfügbarkeit und Einfachheit. Drittens ist es ein zusätzlicher Faktor der Authentifizierung für die erweiterte Sicherheit. Laut Gartner wird dieser Bereich augrund der vielen Optionen von Technologien und Geschäftsmodellen sowie regulatorischen Anforderungen und lokalen Bedingungen ein stark fragmentierender Markt sein,[28] was sich für eine breite Akzeptanz von Mobile Payment negativ auswirken könnte.[29] Deshalb sollen die Marktteilnehmer solche Mobile Payment Systeme entwickeln und anbieten, die von Fall zu Fall die unterschiedlichen Anforderungen, insb. die des mobilen Users erfüllen.[30]

---

24 Vgl. Gartner (2009b).

25 Vgl. Keles (2006), S. 5ff.; Robben (2001).

26 Das Thema Mobile Payment wird in den nächsten Abschnitten näher erläutert. In diesem Stadium wird zunächst in das Thema Mobile Payment eingeleitet.

27 Vgl. Gartner (2009b).

28 Vgl. Ebenda.

29 Vgl. Reder (2009).

30 Die Anforderungen des mobilen Users werden im Abschnitt 3.2.4.1 Anforderungen der mobilen User, S. 72 sowie die Anforderungen der Marktteilnehmer im Abschnitt 3.2 Interessen und Anforderungen der Marktteilnehmer erläutert, S. 63.

2.1.4 Near Field Communication Services

Near Field Communication (NFC) ermöglicht kontaktlose Datenübertragung zwischen kompatiblen Geräten, die zueinander innerhalb von 10 cm nah platziert sind.[31] Dies kann z. B. zwischen einem Mobilfunkgerät und einer Ticket-Verkaufsautomat geschehen. Die NFC-Technologie kann beispielsweise im Einzelhandel, ÖPNV, Personenidentifikation etc. verwendet werden. In der NFC-Technologie sieht man großes Potential für die Erhöhung der Kundenloyalität für die Service Provider beispielsweise für die Luftfahrtgesellschaften. Allerdings besteht hier eine große Herausforderung, eine Vereinbarung zwischen den Mobilfunknetzbetreibern, Service Providern sowie Banken und Transportunternehmen zu erreichen.[32] Jedoch wird sich die breite Akzeptanz der NFC-Services in engen Grenzen halten, solange zu wenige Angebote zur Verfügung stehen, die einen Kundennutzen bringen. Bisher blieb ein Erfolg der NFC-Technologie aus.[33] Laut Gartner wird erwartet, dass sich NFC erst ab dem Ende 2010 entfalten wird, wenn Mobilfunkgeräte mit NFC in großem Umfang an die User gebracht werden.[34] Eng verbunden mit den NFC-Services sind die Contactless Payments (kontaktlose Zahlungen), die im Folgenden näher betrachtet werden.

2.1.5 Contactless Payments

Die neueste Form des bargeldlosen Zahlungsverkehrs sind die Contactless Payments.[35] Die Contactless Payments werden weltweit meistens in den Einzelhandelsgeschäften sowie in öffentlichen Nahverkehrsverbünden verwendet. Die mobilen User können mit einer Smartkarte, Schlüsselanhänger oder Mobiltelefon ihre Einkäufe bezahlen, indem sie ihre Mobiltelefone nahe an einem Terminal oder Lesergerät halten. Diese Smartkarten oder Mobiltelefone sind mit der RFID-Technik ausgestattet.[36] Der Terminal oder das Lesegerät liest die kontaktlose Karte oder das Mobiltelefon und verbindet sich zu einem entsprechenden Kreditinstitut und autorisiert die Zahlungstransaktion. Nach der Autorisierung schließt der User die Zahlungstransaktion. Laut der Anbieter von Contactless Payments können die Zahlungstrans-

---

31 Die NFC-Technologie wird im Abschnitt 2.6.2.1 Near Field Communication, S. 36 näher erläutert.

32 Vgl. Gartner (2009b).

33 Vgl. Reder (2009).

34 Vgl. Gartner (2009b).

35 Vgl. Ezell (2009), S1ff.

36 Die RFID-Technik wird später im Abschnitt 2.6.2.1 Near Field Communication, S. 36 näher erläutert.

aktionen doppelt so schnell wie eine Debit- oder Kreditkarte bearbeitet werden. Es wird erwartet, dass Contactless Payments aufgrund der Einfachheit der kleinen Zahlungstransaktionen mehr genutzt werden.[37] Allerdings bestehen ernsthafte Bedenken von Identitätsdiebstahl und Möglichkeiten der betrügerischen Manipulation.[38]

Ein erster Anwender von Contactless Payments war der Ölkonzern ExxonMobil in den USA, der seit 1997 an den Exxon- und Mobil-Tankstellen das kontaktlose Zahlungssystem „Speedpass“ anbietet.[39] Die Großbanken wie Citibank und Kreditgesellschaften wie Mastercard bieten auch ihre eigene Contactless Payments. Beispiele sind Visa Paywave[40] und MasterCard Paybass[41], die in den USA und in Großbritannien angeboten werden. Die Mobilfunknetzbetreiber haben ebenfalls begonnen, mit der Anwendung der NFC-Technologie Contactless Payments anzubieten.[42] Ein Beispiel ist Belgacom’s Pingping, ein gespeichertes Wert-Konto über eine Partnerschaft mit Alcatel-Lucent Touchatag.[43]

2.1.6 Mobile Marketing

Mobile Marketing wird von der Mobile Marketing Association (MMA) als eine Reihe von Geschäftsaktivitäten definiert, die es Organisationen ermöglicht, sich mit ihrem Publikum in einer interaktiven und relevanten Weise über die Mobilfunkgeräte und mobilen Netzwerke zu kommunizieren und zusammenzuarbeiten.[44] Das Ziel des Mobile Marketing ist es, eine nachhaltige Kundenbeziehung aufzubauen. Danach werden die Marketingmaßnahmen durch die Nutzung mobiler Netzwerke und Mobilfunkgeräte so gestaltet, dass die mobilen User möglichst direkt erreicht werden können, um die Aufmerksamkeit der mobilen User zu erwecken und damit zu einem (Kauf-)

---

37 Vgl. mit dem Abschnitt 2.4 Mobile Payment Typen S. 23.

38 Vgl. Deloitte & Touche LLP (2008).

39 Vgl. https://www.speedpass.com/forms/frmSpHome.aspx, Stand: 25.10.2009.

40 Vgl. http://www.visa.de/ueber_visa/presse/archiv/2007_visa_paywave_europa.jsp, Stand: 25.10. 2009.

41 Vgl. http://www.mastercard.com/us/personal/en/aboutourcards/paypass/, Stand: 25.10.2009.

42 Die NFC-Technologien werden später im Abschnitt 2.6.2.1 Near Field Communication, S. 36 näher erläutert.

43 Vgl. http://wirelessfederation.com/news/16344-belgcoms-pingping-alcatel-lucent-ink-partnership-for-contactless-cards-belgium/, Stand: 18.09.2009.

44 Vgl. MMA Updates Definition of Mobile Marketing, http://mmaglobal.com/news/mma-updates-definition-mobile-marketing, Stand: 11.01.2010.

Verhalten zu führen.[45] Im Mobile Marketing werden maßgeschneiderte Angebote beispielsweise digitale Inhalte wie Musikstücke, Spiele, Videos etc. und Informationen wie News, Produktinformationen unterbreitet. Dabei wird die Erlaubnis der mobilen User für solche Services geholt.[46] Der Trend Mobile Marketing ist eng mit dem zuvor dargestellten Trend, den LBS verbunden. Damit werden die mobilen User über die Produkte und Angebote am Standort informiert.[47] Bei Mobile Marketing verliert der User seine Anonymität, da er seine personenbezogene Daten sowie Standort- und Zeitdaten an die Anbieter der Mobile Marketing Services preisgibt. Es gibt Vorschläge, wie z. B. im Projekt „MoMa-Mobiles Marketing“, wie die User-Anonymität in Mobile Marketing gewahrt werden kann.[48]

2.1.7 Mobile Social Networking

Mobile Social Networking sind soziale Netzwerke, in denen die mobile User ähnliche Interessen und Gemeinsamkeiten haben und sich über die Mobilfunkgeräte austauschen, z. B. Facebook und MySpace.[49] In den Gruppen der User werden viele Transaktionen getätigt. Es ist auch sinnvoll, dass die mobilen User sozialer Netzwerke in der Lage sein können, Geld über das Netzwerk zu senden bzw. zu empfangen. Sie müssen kein Bankkonto haben, sondern nur ein Mitglied in einem sozialen Netzwerk sein. Das ist eine sehr interessante Einnahmequelle für die Anbieter der sozialen Netzwerke. Hier wird z. B. vorgeschlagen, dass die User Geld auf die Konten der sozialen Netzwerke einzahlen, die dann das Geld managen und z. B. Zinsen für diese Gelder erhalten.[50] Danach können soziale Netzwerke das Konto des Users für jede Transaktion mit einem Kleinbetrag (z. B. 5 Cent pro Transaktion) belasten. Auf diese Weise können soziale Netzwerke eigene Mobile Payments anbieten oder als eine Bank auftreten.[51] Einige Soziale Netzwerke wie Facebook oder das niederländische Soziale Netzwerk Hyves haben einen Anfang in Mobile Payments in sozialen Netzwerken gemacht.[52] Facebook experimentiert mit dem Mobile Payment

---

45 Vgl. Graf (2008), S. 3ff.

46 Vgl. Ebenda, S. 4.

47 Vgl. mit dem Abschnitt 2.1.2 Location Based Services, S. 14.

48 Vgl. Bulander/Schiefer/Decker (2005), S. 87ff sowie ausführliche Informationen für das Projekt „MoMa“ unter http://www.aifb.kit.edu/web/MoMaTIK, Stand: 27.10.2009.

49 Vgl. Kharif (2006) sowie http://www.facebook.com/ und http://www.myspace.com/.

50 Vgl. De Laive (2009a).

51 Vgl. Ebenda.

52 Vgl. De Laive (2009b) und Harnick (2009) sowie http://www.hyves.nl/.

Service von Zong[53] und möchte seine Mobile Plattform um Mobile Payment Service erweitern.[54] Hier werden Kredite den Usern gegeben, die dann für z. B. Geschenke, Postkarten etc. verwendet werden.[55] Die niederländische Hyves zielt darauf ab, mit den kommerziellen Transaktionen zwischen den Service Providern und den Usern zu verdienen.[56]

Zusammenfassend kann festgehalten werden, dass die mobilen User gegenwärtig und in der Zukunft immer mehr mobile Services über die Mobilfunkgeräte bzw. mobile (soziale) Netzwerke erhalten bzw. nutzen werden. Die Bezahlung dieser mobilen Services wird ebenfalls über die mobilen Netzwerke durchgeführt werden. Parallel zu diesen Entwicklungen gibt es auch Bedenken und Kritik über die User-Anonymität, die personenbezogenen Daten bzw. Schutz der Privatsphäre. Auf diese Problematik wird in den nächsten Kapiteln eingegangen. Zunächst soll im Folgenden der Begriff Mobile Payment definiert und die Einordnung dieses Begriffs erläutert werden.

2.2 Begriffliche Einordnung und Definition von Mobile Payment

In der Abbildung 2, S. 20 werden die Begriffe, die in der Literatur und der Praxis verwendet werden, in einer Begriffsmatrix nach der Ebene ihrer Prozesse und Technologien eingeordnet. Auf der Ebene der Prozesse (1. Spalte in der Matrix) werden die einzelnen Begriffe Business, Commerce und Payment dargestellt, wobei der Begriff „Business“ der übergreifende Begriff ist und die Begriffe „Commerce“ und „Payment“ umfasst. Andererseits werden auf der Ebene der Technologien (1. Zeile in der Matrix) die einzelnen Bereiche „Electronic“ und „Mobile“ dargestellt, wobei unter dem Begriff „Electronic“ als stationär zu verstehen ist. Der Begriff „Electronic“ bezieht sich auf die stationären Anwendungen, während sich der Begriff „Mobile“ auf die mobilen Anwendungen bezieht.

Nachdem die Ebenen von einzelnen Prozessen und Technologiebereichen eingeordnet sind, werden die Kombinationen von einzelnen Begriffen und Bereichen gebildet. Stationäre Anwendungen in verschiedenen Prozessen werden als Electronic Business, Electronic Commerce und Electronic Payment bezeichnet.

---

53 Vgl. http://www.zong.com/zong/, Stand: 17.02.2010.

54 Vgl. Harnick (2009).

55 Vgl. Ebenda.

56 Vgl. De Laive (2009b).

Mobile Anwendungen in verschiedenen Prozessen werden dagegen als Mobile Business, Mobile Commerce und Mobile Payment bezeichnet.

Technologie / Prozess	Electronic	Mobile
Business	Electronic Business	Mobile Business
Commerce	Electronic Commerce	Mobile Commerce
Payment	Electronic Payment	Mobile Payment

Abbildung 2: Begriffsmatrix

In der Abbildung 3, S. 21 werden die einzelnen Begriffe, die zuvor in der Begriffsmatrix gezeigt wurden, nach dem Umfang und der Dimension der einzelnen Anwendungen sowie deren Beziehungen miteinander dargestellt. Danach können die Begriffe „Electronic Payment“ und „Mobile Payment“ unterschieden werden.

In dem EZB (Europäische Zentralbank) Bericht vom November 2004 wird das Electronic Payment wie folgt definiert:[57]

"*E-Payments sind Zahlungen, die auf elektronischem Wege initiiert, verarbeitet und empfangen werden…*“

Der Begriff Mobile Payment, der auch als mobiles Bezahlen verstanden wird, wird in der Literatur und Praxis unterschiedlich definiert. In der Praxis, d. h. unter den Mobilfunknetzbetreibern, Finanz- und Kreditinstituten und Analysten herrscht zwar keine allgemein akzeptierte Definition von Mobile Payment. Es wird aber einfach als *„Basisdienst für die Abwicklung von elektronischen Zahlungstransaktionen zwischen zwei Peers (Mensch oder Maschine) durch die Nutzung von Mobiltelefonen“* verstanden.[58]

Mobile Payment wird in der Literatur zum Mobile Commerce allgemein definiert als

„diejenige Art der Abwicklung von Bezahlvorgängen, bei der im Rahmen eines elektronischen Verfahrens mindestens der Zahlungspflichtige mobile Kommunikations-

[57] Vgl. ECB Report 2004, S. 7.

[58] Vgl. Andreoli (2008), S. 1.

techniken (in Verbindung von mobilen Endgeräten) für Initiierung, Autorisierung oder Realisierung der Zahlung einsetzt."[59]

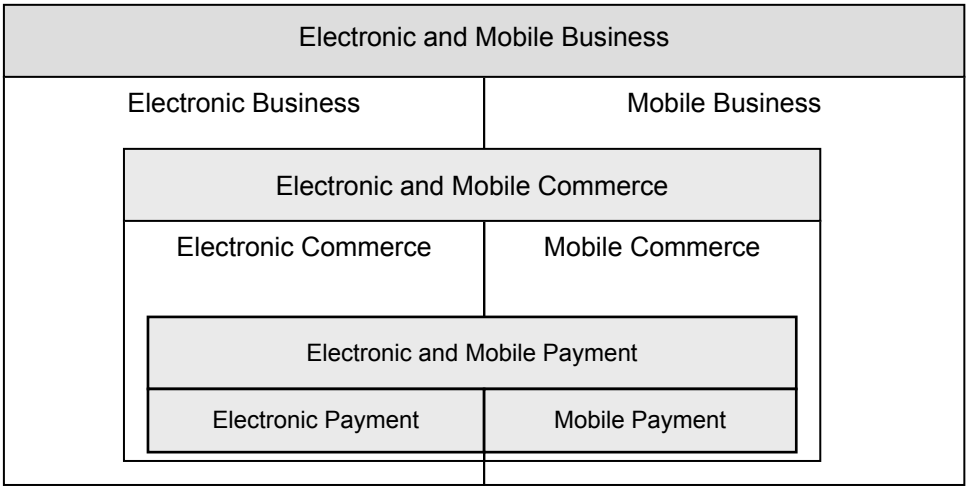

Abbildung 3: Einordnung der Begriffe in die Thematik Electronic und Mobile Business[60]

Mobile Payment ist eine Untergruppe von Electronic Payment, wenn elektronische Zahlungen mit Hilfe mobiler Endgeräte wie Handy, Smartphone etc. getätigt werden. Nach der Definition und der Einordnung stellt der Begriff „Mobile Payment" eine mobile Anwendung für die mobilen Zahlungstransaktionen im Mobile Business und Commerce dar. In der Definition von Mobile Payments, sowohl in der Praxis als auch in der Literatur, wird betont, dass die eingesetzten Mobilgeräte entscheidend für Mobile Payments sind.[61]

Aus den vorigen Definitionen und Ausführungen kann der Begriff Mobile Payment abgeleitet werden. Danach kann Mobile Payment als die Abwicklung der elektronischen Zahlungstransaktionen zwischen zwei Teilnehmern (Mensch oder Maschine) in Mobile Commerce Prozessen sowohl im Nahbereich (Near Field oder POS) als auch im Fernbereich (Remote) durch die Nutzung der Mobilfunkgeräte wie Mobiltelefone, Smartphones oder PDAs definiert werden, wobei die Mobilfunkgeräte für die Initiierung, Verarbeitung und Komplettierung elektronischer und mobiler Zahlungstransaktionen eine integrale Rolle spielen.[62]

---

59 Vgl. Pousttchi (2005), S. 21.

60 In Anlehnung an Link (2003a), S. 4ff. und Link (2003b) S. 5ff.

61 Vgl. Choi et al. (2007), S. 4; Jones (2008).

62 Vgl. mit den Ausführungen im Abschnitt 2.6 Technologien von Mobile Payment Systemen, S. 30 sowie im Abschnitt 2.7 Anwendungsbereiche von Mobile Payments, S. 41.

2.3 Stellenwert von Mobile Payment im M-Commerce

Durch die mobilen (GSM-)Netzwerke können weltweit zurzeit ca. 80 % der Weltbevölkerung von ca. 6,8 Milliarden Menschen abgedeckt werden.[63] Über 3 Milliarden (ca. 45 %) der Weltbevölkerung haben Zugang zu Mobilen Netzwerken.[64] 67 % der Mobilfunkuser leben in Entwicklungsländern. Mobile Payment ist eine sehr wichtige Applikation für Mobile Commerce. Ohne Abrechnung der mobilen Dienstleistungen ist kein M-Commerce möglich. Mobile Payments können fast überall auf der Welt genutzt werden. Weltweit nutzten 2009 ca. 73,4 Millionen User Mobile Payments, dies bedeutet ein Wachstum von 70 % gegenüber 2008 (43,1 Millionen User). Gartner prognostiziert, dass die Zahl der Mobile Payment User bis 2012 auf mehr als 190 Millionen steigen wird.[65] Die User der Mobile Payments tätigten 2,5 Milliarden Zahlungstransaktionen in 2008.[66] Ein überwiegender Teil der mobilen Zahlungstransaktionen wird im asiatischen Raum, vor allem in Japan abgewickelt.[67] Die Nutzung der Mobile Payment wächst auch in afrikanischen Ländern, vor allem in Kenia.[68] Dies wird unter Mobile Remittance im Abschnitt 2.7.4 Mobile Remittance, S. 46 näher erläutert.

Gartner erwartet auch, dass Mobile Payment hinsichtlich der Useranzahl und des Transaktionsvolumens bis 2012 einen großen Marktanteil im asiatisch-pazifischen Raum und in Japan noch beibehält. Außerdem wird prognostiziert, dass die Marktpenetration der Mobile Payments in Westeuropa von 0,9 % in 2009 auf 2,5 % in 2012, in Nordamerika von 1,7 % auf 3 %, im asiatisch-pazifischen Raum und Japan von 2 % auf 3,8 % und in Osteuropa, dem Mittlerem Osten und Afrika auf 3 % bis 2012 steigen wird.[69]

Diese Entwicklung im Mobile Payment zeigt auch das Potential und die Bedeutung von Mobile Payment für M-Commerce. Mobile User möchten einfache, kostengünstige und sichere Zahlungsmöglichkeiten, die sie über ihre Mobiltelefone tätigen können. Händler favorisieren für die Zahlungsabwicklung einfache, kostengünstige

---

63 Vgl. http://www.weltbevoelkerung.de/info-service/weltbevoelkerungsuhr.php?navanchor=1010039, Stand: 12.01.2010.

64 Vgl. http://www.gsmworld.com/technology/services/index.htm, Stand: 12.01.2010.

65 Vgl. Gartner (2009a).

66 Vgl. WPR 2008 (2008), S. 52 und 53.

67 Vgl. Goldhammer (2009); WPR 2008 (2008), S. 52 und 53 sowie Gartner (2009a).

68 Vgl. Haglmüller (2009).

69 Vgl. Gartner (2009a).

und sichere Zahlungssysteme, die möglichst viele Endkunden nutzen können. Es gibt eine Reihe von Mobile Payment Lösungen, jedoch bisher keine standardisierte. Ideal ist eine gemeinsame Lösung für Mobile Payment in und zwischen allen Netzwerken. Derzeit sind Kreditkarten wegen der internationalen Interoperabilität und Akzeptanz die führende Zahlungsmethode.

2.4 Mobile Payment Typen

Mobile Payments werden nach verschiedenen Typen kategorisiert, die wie folgt dargestellt werden können (siehe dazu auch die Abbildung 4, S. 25): [70]

- Mobile Payment nach der Art der Zahlungstransaktion:
    - Pay per view: Mobiler User bezahlt für jede Sicht oder Bestellung abgerufener Inhalte, z. B. Videoclips oder Songs.
    - Pay per unit: Mobiler User bezahlt für jede Einheit abgerufener Inhalte. Die Einheiten können volumen- oder zeitbasiert sein, z. B. Videos nach Volumen (pro Byte oder Megabyte) oder Online Spiele nach Dauer (pro Minute).
    - Pay per flat rate: Mobiler User bezahlt für die unbegrenzten Zugriffe auf die Inhalte in einem Pauschaltarif und einer Periode, z. B. Online Zeitungsartikel.
- Mobile Payment nach dem Zeitpunkt der Zahlungstransaktion:
    - Prepaid: Mobiler User bezahlt für die Inhalte und Produkte im Voraus mit dem Kauf einer Wertkarte oder dem Aufladen eines Guthabenkontos. Der Betrag wird nach jeder Inanspruchnahme der Inhalte abgezogen, z. B. vorausbezahlte Mobilfunkkarten.
    - Paynow: Mobiler User bezahlt schon während des Einkaufs. Die Zahlungstransaktion wird beispielsweise durch ein bankkontenbasiertes System in Echtzeit durchgeführt.

[70] Vgl. McKitterick/Dowling (2003), S. 11ff.; Dannenberg/Ulrich (2004), S. 29ff.

- Postpaid: Mobiler User bezahlt erst nach der Nutzung der Inhalte und Services. Der Betrag wird in Rechnung gestellt und monatlichen mit der Mobilfunkrechnung abgerechnet, z. B. Download von Songs bei einem Mobile Content Provider (MCP).

- Mobile Payment nach der Betragshöhe der Zahlungstransaktion:

  - Micro Payment: Mobiler User kann für die digitalen Inhalte oder für die Services mit der Betragshöhe von bis zu 5 € bezahlen, z. B. Download von Klingeltönen, Logos und Songs etc. oder Parkgebühren.

  - Macro Payment: Mobiler User kann für die digitalen Inhalte oder physischen Produkte mit der Betragshöhe von mehr als 5 € bezahlen, z. B. Online Shopping, Point of Sale etc.

- Mobile Payment nach dem Inhalt der Zahlungstransaktion:

  - Digitale Inhalte und Services: Mobiler User bezahlt für das Herunterladen von Videoclips, Songs und Klingeltönen etc.

  - Physische Produkte: Mobiler User bezahlt für die Waren und Güter im Geschäft oder an Verkaufsautomaten.

- Mobile Payment nach der verwendeten Technologie der Zahlungstransaktion:

  - Remote Mobile Payment: Mobiler User muss bei dieser Art der Zahlungstransaktion nicht persönlich anwesend sein. Bei der Remote Mobile Payment handelt es sich um die Nutzung der Mobile Remote Technologien, z. B. SMS, WAP, USSD, IVR etc.[71]

  - Proximity Mobile Payment: Mobiler User muss bei dieser Art der Zahlungstransaktion persönlich anwesend sein. Bei der Proximity Mobile Payment handelt es um die Nutzung der Mobile Proximity Technologien, z. B. NFC, Bluetooth etc.[72]

---

[71] Diese Technologien werden im Abschnitt 2.6.1 Mobile Remote Technologien, S. 31 näher erläutert.

[72] Diese Technologien werden im Abschnitt 2.6.2 Mobile Proximity Technologien, S. 36 näher erläutert.

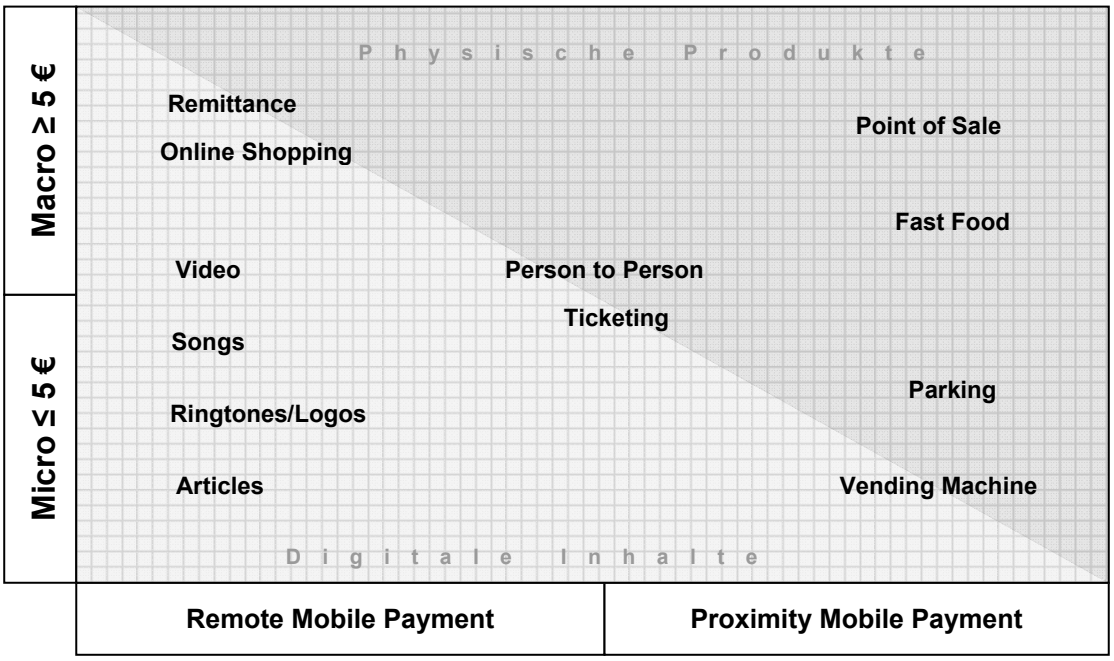

Abbildung 4: Mobile Payment Typen und Güter[73]

In der Abbildung 4 wird diese Kategorisierung mit den Beispielen und eingesetzten Mobile Payment Technologien deutlich gemacht. Die gängigste Kategorisierung für Mobile Payments ist im Allgemeinen die Einstufung nach der Betragshöhe der Zahlungstransaktionen. Danach können Mobile Payments in Micro Payments und Macro Payments unterteilt werden. Micro Payments eignen sich für die Bezahlung digitaler Inhalte oder mobiler Dienstleistungen bis zu € 5-Beträgen. Macro Payments hingegen werden für die Bezahlung der digitalen und physischen Güter im Wert von mehr als 5 € genutzt. Allerdings wird diese Unterscheidung anhand der 5 €-Grenze in der Praxis nicht einheitlich genutzt. Diese Betragsgrenze wird manchmal auch mit 10 € angesetzt.[74] In der Praxis erfolgt häufig auch die Unterscheidung nach dem Zeitpunkt der Zahlungstransaktion.[75]

2.5 Klassifikation von Mobile Payment Systemen

Für die Abrechnung und Bezahlung digitaler Inhalte und mobiler Dienstleistungen werden verschiedene Mobile Payment Systeme angeboten, für die von Banken, Kre-

---

[73] In Anlehnung an Schuba (2004), S. 5ff. sowie Mobey Forum (2003), S. 11 und 14; Sekino/Kwon/Bong (2007), S. 3ff.

[74] Vgl. McKitterick/Dowling (2003), S. 12 sowie Mobey Forum (2003), S. 11.

[75] Vgl. Illik (2002), S. 184.

ditgesellschaften, Mobilfunknetzbetreiber und innovativen Anbietern verschiedene Technologien und Infrastrukturen eingesetzt werden. Die Klassifikation von Mobile Payment Systemen erfolgt deshalb unter den Gesichtspunkten der eingesetzten Technologien, vorhandenen und neuartigen Infrastrukturen und involvierten Teilnehmern.

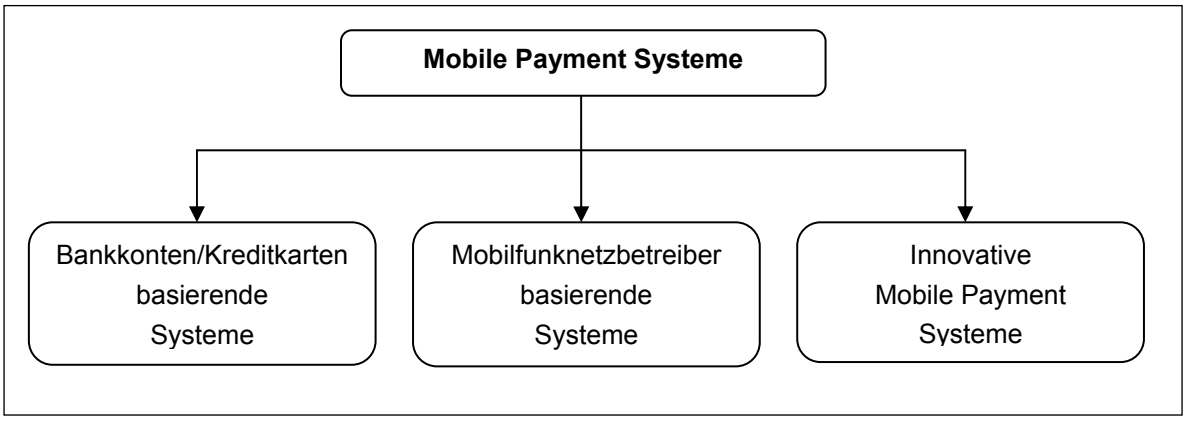

Abbildung 5: Klassifikation von Mobile Payment Systemen nach Infrastrukturen

Die Abbildung 5 zeigt eine Übersicht der Mobile Payment Systeme nach Infrastrukturen, die im Folgenden näher erläutert werden.[76]

2.5.1 Bankkonten und Kreditkarten basierende Mobile Payment Systeme

Bei Bankkonten basierenden Mobile Payment Systemen muss der mobile User für das Bezahlen digitaler Inhalte und mobiler Dienstleistungen über ein Bankkonto verfügen. Diese Mobile Payment Systeme werden meistens für die Zahlung höherer Beträge (Macro Payments) genutzt. Bei diesen Systemen muss sich der mobile User in der Regel mit seinem Mobiltelefon sowie Mobilfunknetzbetreiber registrieren, um sich für eine mobile Zahlungstransaktion authentifizieren zu lassen. Die Authentifizierung des mobilen Users erfolgt mit der PIN-Eingabe[77], die in der Regel mit einer SMS geliefert wird. Bei der Authentifizierung des mobilen Users wird die mobile Zahlungstransaktion verschlüsselt und digitale Signaturen genutzt.[78] Beispiele sind Crandy, LUUPAY und Paybox etc. In manchen Systemen kooperieren die Banken mit den

[76] Vgl. Carr (2007), S. 2ff.

[77] PIN (Personal Identification Number): Persönliche Identifikationsnummer oder auch Geheimzahl ist eine nur einer oder wenigen Personen bekannte Zahl oder Ziffernkombination, mit der diese sich gegenüber einer Maschine (Server) authentifizieren können. Vgl. Brinker/Scholz (2007), S. 6.

[78] Vgl. McKitterick/Dowling (2003), S. 17.

Mobilfunknetzbetreibern und anderen Marktteilnehmern, z. B. Payez Mobile[79] oder die Kooperation zwischen der Deutsche Bank und Luup International.[80]

Die mobilen Zahlungstransaktionen werden per Überweisung (Push-Zahlungsverfahren)[81] oder Lastschriftverfahren in Form des Einzugsermächtigungsverfahren oder des Abbuchungsverfahren (Pull-Zahlungsverfahren)[82] durchgeführt. Beim Erwerb eines Produktes oder einer Dienstleistung wird das Bankkonto belastet, in dem der Händler eine Zahlungsforderung ans Mobiltelefon des Users schickt und der User dann mit seinem Mobiltelefon die Zahlungstransaktion per PIN-Code autorisiert. Bei einigen Systemen fungiert die Mobilfunknummer des Users gleichzeitig als Bankkontonummer wie z. B. LUUPAY.[83]

Neben den Bankkonten basierenden Mobile Payment Systeme gibt es auch die Kreditkarten basierende Mobile Payment Systeme. Diese Systeme werden für die höheren Beträge (Macro Payments) genutzt. Die auf Kreditkarten basierende Mobile Payment Systeme sind die Kreditkartennummern mit den Mobilfunknummern des Kunden verbunden. Wenn der Kunde mit seinem Mobilfunkgerät eine Mobile Payment Transaktion tätigt, wird sein Kreditkartenkonto belastet und der Zahlungsbetrag beim Empfänger gutgeschrieben. Zwischen den Kreditgesellschaften, Mobilfunknetzbetreibern und Geräteherstellern sind einige Kooperationen entstanden. Dadurch sind für die Endgeräte sog. Dual Slot und Dual SIM Technologien entwickelt worden.[84] Mit der Verwendung von Contactless Chip-Technologien und Dual Slot ist es möglich geworden, dass das Mobiltelefon als Zahlungsinstrument überall benutzt

---

79 Vgl. Clark (2009) sowie http://www.payezmobile.com/uk-index.php, Stand: 17.02.2010.

80 Vgl. Bender (2009).

81 Das ist die Art der Zahlungstransaktion, die beinhaltet, wie bzw. von wem eine Zahlungstransaktion initiiert wird. Danach wird unterschieden in Push- und Pull-Zahlungsverfahren. Push-Zahlungsverfahren besagt, dass der Zahler die Zahlungstransaktion initiiert, in dem er den Zahlungsbetrag über die eingebundenen Zahlungssystembetreiber auf ein Konto des Zahlungsempfängers überweist. Vgl. Reichenbach (2002), S. 11.

82 Das ist die zweite Art der Initiierung der Zahlungstransaktion. Pull-Zahlungsverfahren besagt, dass der Zahlungsempfänger die Zahlungstransaktion initiiert, in dem er seine Bank beauftragt den Zahlungsbetrag über die Bank des Zahlers und vom Konto des Zahlers einzuziehen. Vgl. Reichenbach (2002), S. 11.

83 Der Mobile Payment Anbieter LUUPAY hat am 10.03.2009 seinen Betrieb in Deutschland eingestellt, ist jedoch aktiv als Kooperationspartner der Deutsche Bank sowie anderer Banken und Finanzinstitute weltweit. Vgl. Gajek (2009) sowie die Fußnote 79, S. 27.

84 Vgl. Die Dual Slot, Dual SIM sowie Contactless Chip Technologien werden später im Abschnitt 2.6.2.5 Contactless Konzept - Dual-Chip-Technik, S. 39 erläutert.

werden kann. Gegenwärtig werden auch neue sog. Proximity-Technologien wie NFC entwickelt und in vielen Projekten eingesetzt.[85]

2.5.2 Mobilfunknetzbetreiber basierende Mobile Payment Systeme

Bei den Mobilfunknetzbetreiber basierenden Systemen werden die Mobiltelefone für die Authentifizierung des Users verwendet. Die meisten Mobile Payment Lösungen basieren auf GSM-Netzwerktechnologie. Die Mobilfunknetzbetreiber haben Erfahrung in der Abrechnung von mobilen Telekommunikationsdienstleistungen. Neben den Telekommunikationsdienstleistungen werden auch die Dienstleistungen von Drittanbietern sog. Content Providern abgerechnet und beglichen. Diese Art der Abrechnung und Billing-Systeme werden auch Mobile Billing genannt.[86] Der mobile User erwirbt digitale Inhalte oder andere mobile Dienstleistungen, indem er sein Mobiltelefon nutzt. Danach wird das Konto des mobilen Users bei seinem Mobilfunknetzbetreiber belastet. Der User begleicht seine Mobilfunkrechnung bei seinem Mobilfunknetzbetreiber. Mobile Billings werden entweder über die Prepaid-Konten oder die monatlichen Telefonrechnung von Postpaid-Kunden abgewickelt. Durch sog. Revenue Sharing-Vereinbarungen (Umsatz- und/oder Provisionsverteilung)[87] kooperieren Content Provider und Mobilfunkanbieter, um die Kundenbasis für Telekom- und Content-Dienstleistungen zu erweitern.[88]

Aufgrund der Kompetenz und Erfahrung im Bereich der Abrechnung und Begleichung mobiler Telekommunikationsdienstleistungen sowie des Betriebs der Infrastrukturen werden die Mobilfunknetzbetreiber als direkter Anbieter von Mobile Payment gesehen. Mobilen Usern werden entweder die Abonnement-Modelle oder Payment pro Nutzungs-Modelle angeboten, in denen meistens kleine Beträge (Micro Payments) abgerechnet werden.[89] Ein Beispiel hierfür ist T-Pay der Deutschen Telekom.

T-Pay ist das Online-Zahlungssystem der Deutschen Telekom, das eine Plattform für mehrere Zahlungsmöglichkeiten darstellt.[90] Neben der Abrechnung per Lastschrift

---

85 Vgl. Heikkinen (2009), S. 10.

86 Vgl. Pousttchi (2003), S. 409.

87 Vgl. Van Bruwaene (2006), S. 4; Pousttchi (2003), S. 412 sowie http://www.answers.com/topic/revenue-sharing, Stand: 28.01.2010.

88 Vgl. Karnouskos (2004), S. 48.

89 Vgl. McKitterick/Dowling (2003), S. 15.

90 Vgl. http://www.t-pay.de/index.html, Stand: 28.01.2010.

und Kreditkarte kann auch über die monatliche Telekom-Rechnung bezahlt werden. T-Pay bietet mit Pay by Call die Möglichkeit, per Telefonanruf (max. eine Stunde) bei einer Servicenummer Beträge zu bezahlen. Außerdem können kleine Beträge (Micro Payments) mit der Guthabenkarte MicroMoney von T-Pay bezahlt werden.[91]

2.5.3 Innovative Mobile Payment Systeme

Neben den vorgestellten Mobile Payment Systemen sind auch innovative Mobile Payment Systeme entstanden, die entweder von im Internet etablierten Firmen wie Google, eBay und Amazon etc. oder von Start-Up's angeboten werden. Diese Systeme benutzen wiederum die Infrastrukturen der Banken und Kreditkartengesellschaften. Die Anbieter wickeln die Zahlungstransaktionen über die Bankkonto, Kreditkartenkonto, Guthabenkonto (Wertkarte oder Gutschein) des Users oder per Rechnung ab. Der User benötigt für die Nutzung des Mobile Payment Services seine Bankverbindung und Kreditkartennummer sowie in der Regel eine Registrierung beim Mobile Payment Anbieter. Die innovativen Systeme werden in unterschiedlichen Mobile Payment Typen eingesetzt.

Amazon.com bietet ein Payment System mit Amazon Payments (Checkout by Amazon, Amazon Simple Pay sowie 1-Click Checkout) an.[92] Google bietet Google Checkout in den USA und Großbritannien an und ist jedoch noch nicht so erfolgreich wie die Konkurrenzangebote von eBay und Amazon. Google Checkout funktioniert mit Kreditkarten für Macro Payments. Der Online-Auktion-Anbieter eBay bietet seinen Mobile Payment Service PayPal Mobile an. PayPal Mobile basiert auf Bank- oder Kreditkartenkonto. Mit PayPal Mobile können die Beträge im Bereich Micro und Macro Payments bezahlt werden. Paypal Mobile kann auf verschiedenen Mobilfunkplattformen wie iPhone, Android und Blackberry verwendet werden. Amazon Payments, Google Checkout und PayPal Mobile, alle drei Mobile Payment Dienste sind die Erweiterung ihrer existierenden Online-Zahlungsmethoden im Internet. Sie bieten jedoch auch Mobile Payment Services an. Der mobile User muss sich bei diesen Systemen registrieren und eine PIN-Nummer einrichten lassen, die dann verwendet wird, um alle Einkäufe oder Zahlungen zu verifizieren.[93]

PayPal und Twitter bieten in einer Kooperation das Mobile Payment Verfahren Twitpay an, wobei die Zahlungstransaktionen über PayPal Mobile abgewickelt

---

91 Vgl. http://www.t-pay.de/t-pay-info/shoppen-mit-micromoney.html, Stand: 28.01.2010.

92 Vgl. https://payments.amazon.com/sdui/sdui/index.htm, Stand: 28.01.2010.

93 Vgl. http://www.gomonews.com/top-5-mobile-payment-services/, Stand: 26.02.2010.

werden.[94] Twitpay gilt als ein Social Payment (oder auch Social Micropayment) Verfahren, das die Bezahlung der Inhalte (Micro Payments) und die P2P-Zahlungen in Social Networks wie Twitter, Facebook etc. ermöglicht. Die Privatsphäre bzw. Anonymität des Users werden in solchen Verfahren wie z. B. in Twitpay nicht ganz gewährleistet. Wenn der User Geld sendet oder empfängt, wird eine Twitter-Nachricht[95] gesendet. So kann jeder in einer Social Network-Gruppe die einzelnen Zahlungen eines jeden Users sehen bzw. verketten.[96] Darüber hinaus gibt es neue Social Payment-Dienste wie z. B. Flatter. Flatter ist ein Social Micropayment-Dienst für die Abrechnung der Inhalte oder Beiträge von Usern in Social Networks auf einer Spendenbasis.[97]

2.6 Technologien von Mobile Payment Systemen

Für die technische Gestaltung von Mobile Payment Systemen werden verschiedene mobilen Telekommunikationsnetzwerk- und Dienstleistungstechnologien verwendet. Im Bereich mobiler Netzwerktechnologien sind einige Technologiegenerationen entstanden, die in der Abbildung 6, S. 31 dargestellt werden. Im Bereich von Mobile Payment wird basierend auf mobilen Netzwerktechnologien eine Reihe mobiler Dienstleistungstechnologien eingesetzt, die wie in der Abbildung 7, S. 32 dargestellt in zwei Gruppen unterteilt werden können. Danach gibt es Mobile Remote Technologien und Mobile Proximity Technologien, die bei der technischen Gestaltung von Mobile Payment Systeme zum Einsatz kommen.[98] Viele Mobile Payment Technologien konkurrieren miteinander, um sich auf dem Markt von Mobile Payment als Standards zu etablieren. Die Mobile Payment Technologien bestimmen die User-Anonymität und sind sehr wichtig für deren Gestaltung in Mobile Payment Systemen. Deshalb sollen im Folgenden die einzelnen Mobile Payment Technologien sowie die Beeinflussung der User-Anonymität durch die Verwendung dieser Technologien erläutert.

---

94 Vgl. Scholz (2008); https://twitpay.me/p/faq, Stand: 26.02.2010.

95 Twitter ist ein Nachrichtendienst, der als soziales Netzwerk den angemeldeten Usern Senden und Empfangen kurzer Textnachrichten (mit max. 140 Zeichen) ermöglicht. Vgl. O'Reilly/Milstein/Lang (2009), S. 7.

96 Vgl. http://www.squidoo.com/twitter-micropayments, Stand: 26.02.2010; Twitter wird u. a. auch wegen der Privatsphäre bzw. des Datenschutzes heftig kritisiert. Vgl. Schonschek (2009).

97 Vgl. Weigert (2010); Vatter (2010).

98 Vgl. Jones (2008), S. 3ff.; Jain/Seri/Srinivasan (2008), S. 16ff.

Generation	Technik	Übertragung	Bandbreite im Download
1G	AMPS	analog, leitungsvermittelt	-
2G	GSM	digital, leitungsvermittelt	9,6 kBit/s
2.5G	HSCSD	digital, leitungsvermittelt	57,6 kBit/s
	GPRS	digital, paketvermittelt	115 kBit/s
2.75G	EDGE	digital, paketvermittelt	236 kBit/s
3G	UMTS	digital, paketvermittelt	384 kBit/s
3.5G	HSPA	digital, paketvermittelt	14,4 MBit/s
4G	WiMAX	digital, paketvermittelt	20 MBit/s
	LTE	digital, paketvermittelt	100 MBit/s

Abbildung 6: Generationen der Mobilfunktechnologien[99]

2.6.1 Mobile Remote Technologien

In einem drahtlosen mobilen Netzwerk stehen den mobilen Usern verschiedene mobile Remote (ferne) Dienstleistungen zur Verfügung. Der mobile User muss in einer Remote-Transaktion nicht physisch oder persönlich anwesend sein. Die mobilen Remote Dienstleistungen sind beispielsweise Abruf von Informationen, Location Based Services, Mobile Payment und Mobile Banking bei spontanen Einkäufen von digitalen Inhalten und Dienstleistungen. Solche mobile Transaktionen werden in der Regel durch menügesteuerte Anwendungen realisiert. Die mobilen Remote Dienstleistungen werden meistens von den Mobilfunknetzbetreibern und Content Providern angeboten. Bei den mobilen Remote Dienstleistungen werden die Billing und Account-Systeme von Mobilfunknetzbetreiber genutzt. Die wichtigsten Remote Mobile Technologien sind SMS, WAP, USSD, IVR, J2ME etc. Diese Technologien werden im Folgenden erklärt.

[99] Vgl. http://www.elektronik-kompendium.de/sites/kom/0406221.htm, Stand: 28.01.2010.

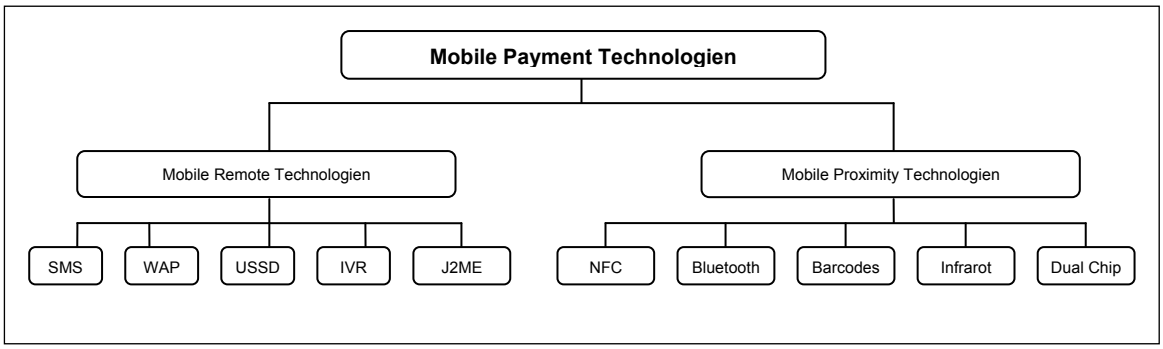

Abbildung 7: Mobile Payment Technologien

2.6.1.1 SMS/Text Messaging

SMS (Short Message Service) oder Text Messaging ist eine Technologie zum Senden und Empfangen von Textnachrichten mit einem Mobilfunkgerät. Der SMS-Dienst wurde ursprünglich in 1992 als Textinformationen zusätzlich zu Sprachinformationen in der GSM-Technologie gedacht.[100] Dies ist zunächst meistens kostenlos angeboten worden und wurde unter den Mobilfunkkunden sehr schnell beliebt.[101] Später jedoch wurde der SMS-Dienst aufgrund seiner ökonomischen Bedeutung kostenpflichtig.[102] Neben der einfachen Übermittlung von Textnachrichten zwischen Personen haben sich neuartige Serviceinformationen wie News, Börse, Wetter und Sport etc. entwickelt.[103] Diese Serviceinformationen (Premium SMS) werden meistens durch MCP angeboten. Der Premium SMS dient als Abrechnungsmöglichkeit im Micro Payment Bereich. Die Kosten der Premium SMS Services erscheinen dann am Monatsende auf der Mobilfunkrechnung. Laut Gartner wurden 2007 in Westeuropa 202 Milliarden SMS (in 2009 215 Milliarden SMS prognostiziert) geschickt.[104] Das weltweite Volumen belief sich in 2008 auf 2,3 Billionen SMS.[105] Der SMS-Dienst ist heute und voraussichtlich bis 2011 die dominierende Mobile Payment

---

[100] Vgl. Zerfos et al. (2006), S. 1 sowie http://www.iec.org/online/tutorials/acrobat/wire_sms.pdf, Stand : 28.01.2010.
GSM steht für Global System for Mobile Communications (Globales System für mobile Kommunikation), ist ein weltweit anerkannter Standard für digitale Mobilfunk-Kommunikation. Mehr Informationen über GSM-Technologie unter http://gsmworld.com/technology/gsm/index.htm, Stand: 28.01.2010.

[101] Vgl. Trappe (2007), S. 9.

[102] Vgl. Ebenda.

[103] Vgl. McKitterick/Dowling (2003), S. 6.

[104] Vgl. Gartner (2007).

[105] Vgl. Ebenda.

Technologie.[106] Die Nutzung der SMS bzw. MMS Technologie gewährleistet den mobilen Usern keine Anonymität.

2.6.1.2 WAP

Der WAP (Wireless Application Protocol) ist eine Technologie zur Übertragung und Darstellung von Internet-Inhalten und mobilen Anwendungen und Diensten auf den Mobilfunkgeräten. Die Mobilfunkgeräte kommunizieren bei WAP-Anwendungen nicht direkt mit den Webservern sondern über ein WAP-Gateway.[107] Der WAP-Gateway übersetzt die Anfragen vom Mobilfunkgerät in eine http-Anfrage und leitet diese an die Webserver. Die Internet-Seiten werden auf dem Mobilfunkgerät als WML-Seiten (Wireless Markup Language) dargestellt. WML ist eine Programmierungssprache ähnlich wie HTML und ermöglicht die Darstellung von einfachen und formatierten Texten, Tabellen und Bildern in sog. Microbrowsern für ein Mobilfunkgerät, z. B. Opera Mini, Opera Mobile, Klondike und WinWAP etc.[108]

Die WAP-Technologie wird für die Nutzung und Abrechnung verschiedener Dienste (WAP-Billing, z. B. Payforit) eingesetzt.[109] WAP-Billing ermöglicht Usern digitale Inhalte und Dienste über das Mobilfunkgerät zu zahlen. Solche Dienste sind News, Wetter-Infos, Entertainment, Banking, Stadt- und Parkinformationen und ÖPNV etc.[110] Mit einem WAP-fähigen Mobilfunkgerät können User ohne Probleme verschiedene Internetinformationen und -dienste in Anspruch nehmen. Aufgrund der relativ geringen Datenübertragungsgeschwindigkeit und geringeren Displaygröße der WAP-Endgeräte werden jedoch nur ausgesuchte Inhalte und keine vollständigen Internetseiten dargestellt und deshalb sind spezielle Anpassungen der Inhalte erforderlich.[111]

---

106 Vgl. Gartner (2008).

107 Vgl. Mielke (2002), S. 191.

108 Vgl. http://www.ccwap.de/WAP_einfuehrung_%206.htm und http://www.wapgprs.de/index_2.html sowie http://www.mobile-times.ch/database/Heft17/17_32_34.html, Stand: 28.01.2010.

109 Vgl. http://www.portel.de/nc/nachricht/artikel/41620 und http://www.payforituk.com/index.html, Stand: 28.01.2010.

110 Vgl. http://www.iec.org/online/tutorials/acrobat/wap.pdf, S. 3, Stand: 28.01.2010.

111 Vgl. Dulz (2005); Alby (2008), S. 21.

2.6.1.3 USSD

Die USSD (Unstructured Supplementary Service Data) ist eine Technologie zum Senden und Empfangen von Kurztextnachrichten zwischen Mobilfunkkunden und dem Netz ähnlich wie bei SMS. Jedoch unterscheidet USSD sich von SMS dadurch, dass sich es bei SMS um eine „store and forward" Technik[112] handelt, die eine SMS-Nachricht zuerst zum SMS-Center vom Sender schickt, bevor diese Nachricht an den Empfänger gesendet wird. Der Sender erhält nur eine Empfangsbestätigung vom SMS-Center. Es ist auch nicht immer garantiert, dass die gesendete SMS-Nachricht sofort den Empfänger erreicht.[113]

Im Gegensatz zu SMS wird eine USSD-Nachricht vom Mobilfunkgerät des Users sofort an die Applikationsplattform von USSD-Service gesendet. Somit wird eine Real-Time (Echtzeit)-Verbindung zwischen dem User und der Applikationsplattform von USSD-Service initiiert. Der User kann dann Informationen senden und empfangen, bis ein USSD-Service komplett ist. Die Real-Time-Verbindung hat bei interaktiven menügeführten Applikationen den Vorteil, dass der User mit seinem Mobilfunkgerät einen USSD-Service nutzt, beispielsweise seinen aktuellen Kontostand erfahren oder ein Guthaben aufladen möchte.[114] Beispiele sind Hello Money von Barclays Bank in Indien[115] oder Celcom Aircash[116] in Malaysia. Mit USSD können außerdem interaktive Applikationen und Informationsdienstleistungen wie News, Sportergebnisse und Wetterberichte angeboten werden.[117]

2.6.1.4 IVR

IVR (Interactive Voice Response) ist eine Informationstechnologie, mit der ein Computer Stimmen- und/oder Tastatureingaben von Usern über ein (Mobil-) Telefon

---

[112] Vgl. Bertsch (2001), S. 94; Store and forward (Speichern und Weiterleiten)-Technik ist eine Technologie, die früher von Nachrichtenübermittlungssystemen benutzt wurde, um Nachrichten vorübergehend zu speichern und anschließend an das Zielsystem weiterzuleiten. Die Store-and-Forward-Technologie ist ideal für den Einsatz bei Anwendungen, die keine Echtzeit-Anwendungen sind. Vgl. http://www.bergt.de/lexikon/lex/sl2.htm, Stand: 03.10.2009.

[113] Vgl. Dialogic (2008), S. 2ff sowie http://www.tanlasolutions.com/ussd.htm und http://www.telecom space.com/messaging-ussd.html, Stand: 18.02.2010.

[114] Vgl. Ebenda.

[115] Vgl. http://www.barclays.in/hellomoney/, Stand: 18.02.2010.

[116] Vgl. http://www.celcom.com.my/aircash/Faq.html, Stand: 18.02.2010.

[117] Vgl. http://www.telecomspace.com/messaging-ussd.html, Stand: 18.02.2010.

erkennen kann. Die IVR-Systeme können mit einem Audio-Rekorder mit Usern interagieren. Der User kann durch Tastatur- und/oder Spracheingaben seine Antwort schicken. Typische Anwendungsbeispiele von IVR-Technologie sind Telebanking, Televoting[118] (Abstimmungsverfahren), Kreditkartentransaktionen, Wetterberichte, Identifizierung und Führung von Anrufern sowie Bestellungsanordnungen.[119]

IVR-Systeme werden neben Mobile Payment in mehreren Bereichen wie Telefonbanking, Anruferidentifizierung und routing[120] etc. eingesetzt. IVR-Systeme können dem User erlauben, relativ anonym Daten zu erhalten. Krankenhäuser und Kliniken sowie Pharmaunternehmen benutzen IVR-Systeme, um den Anrufern relativ anonymen Zugang zu den Testergebnissen zu gewährleisten, da die Testergebnisse private und sensitive Information beinhalten.[121] Im Laufe der Zeit entwickelte sich die IVR-Technologie in vier Generationen.[122] Jede Generation der IVR-Technologie hat zu neuartigen Mobilfunkgeräten geführt. Aktuelle Entwicklungen gehen zur Erkennung von Emotionen der User, die auf biometrischen Techniken basieren.[123]

2.6.1.5 J2ME

Java Platform, Micro Edition (Java ME) ist eine Ansammlung von Technologien und Spezifikationen zu einer Plattform, um die Anforderungen von Mobilfunkgeräten wie Consumer Devices, Embedded Devices und erweiterte Mobilendgeräte zu erfüllen. J2ME (Java 2 Plattform, Micro Edition) bietet eine robuste und flexible Entwicklungsumgebung für die Anwendungen, die auf mobilen Endgeräten oder anderen Embedded Devices wie Mobilfunkgeräten, PDAs, Fernseher-Sets und Druckern laufen.[124]

---

118 Vgl. http://www.computerbase.de/lexikon/Televoting, Stand: 28.01.2010.

119 Vgl. die Erläuterungen in http://www.magex.com/content/white_label2.html, Stand: 18.02.2010.

120 IVR-Systeme werden u. a. als dialogorientierte Sprachsysteme zur Entlastung von Routine-Aufgaben und zur Warteschlangenverwaltung in Call Centern eingesetzt. Das Routing bezeichnet dabei die Anrufverteilung zwischen verschiedenen Teams oder räumlichen Einheiten innerhalb des Call Centers. Dabei werden Anrufe an ein Inhouse Center, die dieses nicht mehr in der gewünschten Zeit abarbeiten kann, an einen anderen Standort oder einen externen Dienstleister weitergeleitet, ohne dass der Anrufer dies bemerkt. Vgl. Florl (2001), S. 27 sowie http://www.it wissen.info/definition/lexikon/interactive-voice-response-IVR.html, Stand: 03.10.2009.

121 Vgl. http://www.tiresias.org/research/guidelines/telecoms/ivr.htm, Stand: 18.02.2010.

122 Vgl. Larson (2008), S. 1.

123 Vgl. Ebenda.

124 Vgl. http://java.sun.com/javame/index.jsp, Stand: 03.10.2009.

Die J2ME-Technologien sind speziell für den Consumer-Markt entwickelt worden. Auf diesem Markt sind mobile Endgeräte mit limitierten Ressourcen wie kleines Display, kleine Speichergröße und eingeschränkte Prozessorleistung etc. ausgestattet. Somit haben solche Geräte geringere Kommunikations- und Übertragungsmöglichkeiten als größere Systeme. Um diese Anforderungen zu erfüllen, wird auf bestimmte Java-Funktionen in der J2ME-Entwicklung verzichtet.

2.6.2 Mobile Proximity Technologien

Neben den Remote-Mobile-Technologien sind in letzter Zeit auch die Proximity-Mobile-Technologien aufgetreten. Die mobilen User erhalten die Mobilen Proximity Dienstleistungen bei persönlicher Anwesenheit am Verkaufsort, in dem sie ihre Mobiltelefone nah an einen Verkaufsautomaten oder am Zahlungsterminal halten. Die Beispiele für die Mobilen Proximity Dienstleistungen sind die Bezahlung im öffentlichen Verkehr wie z. B. an den Bahnticketautomaten und Parkhäusern oder die Zugangsberechtigung zu Stadien oder Events.[125] Diese Technologien sind Barcodes (Strichcode), Bluetooth, Infrarot und Short-range Contactless (Kontaktlose Kurzstrecken-) Technologien. Diese Technologien müssen die Anforderungen von User und Service Provider wie z. B. Reichweite, Geschwindigkeit, Sicherheit, Komfort, Vertrauen, Robustheit und Kosten erfüllen.[126] Im Folgenden werden deshalb die wichtigsten Proximity-Mobile-Technologien kurz vorgestellt, mit deren Hilfe eine lokale, nahe Verbindung mit einem Mobiltelefon hergestellt werden kann.

2.6.2.1 Near Field Communication

Die Near Field Communication ist eine Technologie, die von Philips und Sony für die drahtlose Übertragung entwickelt worden ist. Die NFC ist eine Entwicklung der Contactless und der Kurzstrecke-Radiofrequenz-Technik RFID (Radio Frequency Identification). Die NFC-Technologie funktioniert im Bereich von 13,56 MHz bis zu 10 cm Entfernung. Die NFC-Technologie bietet drahtlose Peer-to-peer-Kommunikation und kontaktlose Kartenleser-Funktion und ist für schnelle und bequeme Magnetstreifen- und Berührungstransaktionen wie an Verkaufsautomaten, Ticket- oder

[125] Vgl. Durix (2004), S. 3ff.

[126] Vgl. Ebenda.

Parkautomaten konzipiert.[127] So wird das Mobiltelefon als kontaktlose Smartkarte für die Zahlungstransaktionen im Nahbereich eingesetzt. Beispiele sind RMV-HandyTicket[128] in Deutschland, NTT DoCoMo's "osaifu keitai“ in Japan, Octopus card in Hong Kong und Oyster card in London.[129] Aufgrund der Geschwindigkeit und Sicherheitsfragen wurden die „Secure NFC“ weiterentwickelt, durch die ein direkter Link zwischen NFC-Chip und SIM-Karte hergestellt wird.[130] Jedoch äußern Datenschützer Kritik und Bedenken über die RFID-Technik, da das Kaufverhalten der User detailliert zurückverfolgt werden kann und der User durch das versteckte RFID keine Kontrolle mehr darüber hat, welche Informationen preisgegeben werden.[131]

2.6.2.2 Bluetooth

Bluetooth ist eine Funktechnologie für die Nahbereichübertragung bis 10 m, die mit 2,4 GHz betrieben und zur drahtlosen Kommunikation und Datenaustausch zwischen den mobilen Endgeräten in einem Personal Area Network (PAN) verwendet wird. Ein mobiler User kann damit sein Mobilfunkgerät mit seinem Headset-Gerät, einem Access Point, einem PC oder einem anderen User verbinden, sog. Bluetooth Pairing.[132] Bluetooth ist bereits in zahlreichen Mobilgeräten verfügbar und wird als eine sichere Funktion für die Vernetzung von Geräten im Nahbereich betrachtet.[133]

---

127 Vgl. http://www.itwissen.info/definition/lexikon/Nahfeldkommunikation-NFC-near-field-communication.html, Stand: 03.10.2009.

128 Vgl. http://www.rmv.de/coremedia/generator/RMV/Tickets/RMVHandyTicket/NFC sowie http://mobil.rmv.de/, Stand: 19.02.2010.

129 Vgl. Best (2008).

130 Vgl. Durix (2004), S. 3ff.

131 Vgl. http://www.rfid-chips.net/index.php?option=com_content&task=view&id=18&Itemid=33 Stand: 02.10.2010.

132 Bluetooth Pairing bezeichnet die Überprüfung der Zugangsberechtigung zu einem Piconetz (ein zufälliger, räumlicher Zusammenschluss von zwei bis maximal acht Bluetooth-Geräten) durch Bluetooth-Geräte. Vgl. http://www.dsltarife.net/lexikon/222.html, Stand: 02.10.2009. Wollen zwei Bluetooth-Einheiten zum ersten Mal miteinander in Kontakt treten, müssen sie den Bluetooth Pairing-Prozeß durchlaufen. Ergebnis dieses Prozesses ist ein Verbindungsschlüssel, der in einer Tabelle für weitere Kontaktaufnahmen gespeichert, oder nach der Kommunikation wieder verworfen wird. Speichern die Geräte den Schlüssel, brauchen sie bei erneuter Kontaktaufnahme den Pairing-Vorgang nicht nochmals durchlaufen. Der Verbindungsschlüssel ist der Eingangsparameter für alle sicherheitsrelevanten Mechanismen. http://www.internet-sicherheit.de/service/glossar/eintrag/eintrag-detail/bluetooth-pairing/, Stand: 02.10.2009.

133 Vgl. http://www.all-about-security.de/security-artikel/endpoint-sicherheit/mobile-computing-und-pdas/artikel/282-bluetooth-die-grundlagen/ und http://www.chip.de/artikel/c_druckansicht_12137428.html sowie http://www.bluetooth.com/Bluetooth/Fast_Facts.htm, Stand: 02.10.2009.

Die Bluetooth-Technologie ist gut geeignet, große Menge von Daten zu übertragen, aber nicht konzipiert für die schnelle Übertragung von Daten. Denn es gibt ein Problem in der Geschwindigkeit der Verbindungen, wenn mehrere User gleichzeitig Bluetooth an einem bestimmten Ort einschalten. Danach initialisiert jedes bluetooth-fähiges Gerät eine Kommunikation mit den umliegenden Bluetooth-Geräten und erstellt eine Liste der verfügbaren Geräte für den User zur Bestätigung eines Verbindungsaufbaus. Dies verringert zunehmend die Geschwindigkeit einer Transaktion von mehreren Sekunden.[134]

2.6.2.3 Barcodes

Der Barcode, auch Strichcode genannt, ist eine maschinell optisch lesbare Information und kann als ein numerischer oder alphanumerischer Identifikationscode interpretiert werden.[135] Barcodes werden in der Warenwirtschaft und der Warenauszeichnung, im Transport und in der Lagerhaltung verwendet.[136] Überwiegend wird diese Technologie in der Einzelhandelsbranche eingesetzt, in letzter Zeit auch bei mobilen Anwendungen und Dienstleistungen wie z. B. mobile Ticketing in der Bahn, den Fluggesellschaften oder Veranstaltungen.[137] Ein mobiler User kann unterwegs auf Anfrage den Barcode herunterladen, um beispielsweise einen Zugangsberechtigung zu einem Fußballstadion oder Informationen über Kino oder Theater zu erhalten.[138] Die Barcode-Technologie ist zwar kostengünstig und kann schnell gelesen werden, hat jedoch ein Sicherheitsproblem, da ein Barcode wie ein Bild kopiert werden kann. Daher erfordert die Barcode-Technologie eine parallele Verwendung eines Identitätsnachweises wie bei Kreditkarten.[139] Die Nutzung der Barcode in Mobile Payment Anwendungen bietet keine User-Anonymität, da sich der mobile User beim Service Provider registrieren muss. Außerdem werden Tickets als Bar-

---

134 Vgl. Durix (2004), S. 3ff.

135 Vgl. http://woerterbuch.babylon.com/Barcode sowie http://www.itwissen.info/definition/lexikon/Strichcode-bar-code.html, Stand: 02.10.2009.

136 Vgl. http://www.artikelweb.de/db/artikel_barcode-_und_kennzeichnungs-systeme_fuer_handel_gewerbe_und_industrie.html, Stand: 19.02.2010.

137 Vgl. http://www.spiegel.de/reise/aktuell/0,1518,433377,00.html sowie http://www.heise.de/newsticker/meldung/Fluggaeste-sollen-mit-Barcode-auf-dem-Handy-Display-einchecken-koennen-115736.html, Stand: 02.10.2009.

138 Vgl. http://www.media.nrw.de/media2/site/index.php?id=73&no_cache=1&tx_ttnews[tt_news]=50320&cHash=02eb9c44af, Stand: 19.02.2010.

139 Vgl. Durix (2004), S. 3ff.

code mit einer MMS (Multi Media Message) oder SMS an die Mobilfunknummer des Users geschickt. Der User soll dabei seine Mobilfunknummer nicht unterdrücken.[140]

2.6.2.4 Infrarot

Die Infrarot-Technologie wird verwendet, um u. a. zwei (mobile) Geräte miteinander zu verbinden. Diese Technologie wird in vielen Bereichen angewendet wie z. B. für Fernbedienungsgeräte oder wie bei Kommunikation und Datenaustausch zwischen PC und Peripheriegeräten, PDA und Mobiltelefonen. Die Finanzindustrie nutzt die Infrarottechnologie für die Zahlungstransaktionen im Nahbereich, indem sie den Sicherheitsstandard IrFM (Infrared Financial Messaging) einsetzt.[141] Der Standard IrFM gibt detaillierte Informationen zu User-Anwendungsmodellen und Richtlinien für die Implementierung in Terminals und Mobilgeräten sowie für das Senden und Empfangen von Transaktionen zwischen Kassen- und Mobilgeräten.[142] Viele Mobiltelefone sind mit der Infrarot-Technik ausgestattet. Die Infrarot-Technologie bietet eine akzeptable Geschwindigkeit[143] und gilt gegenüber Bluetooth und WiFi (Wireless Fidelity)[144] als relativ sicher.[145]

2.6.2.5 Contactless Konzept - Dual-Chip-Technik

Für das Contactless-Konzept existieren zwei SIM-Kartenlösungen. Die eine Lösung basiert auf der Twin SIM-Karte (eine Steckkarte mit zwei eingebetteten Chips). Ein Chip ist für die Telefonie, der andere für die Contactless-Applikation. Beide Chips haben in der Regel keine Verbindung miteinander, um alle Daten gemeinsam zu nutzen, können jedoch mit einer Contactless-Schnittstelle verbunden werden. Die Twin-SIM-Kartenlösung findet einige Anwendungen, bei denen zugleich die Anmeldeinformationen und Identifikationsmerkmale von mobilen Usern verwaltet bzw. geprüft werden, wie beispielsweise in der Zugangskontrolle zu Stadien und Events, Mobile Ticketing etc. Die andere SIM-Lösung ist die SIM-Kombikarte mit einem ein-

---

140 Vgl. http://www.spiegel.de/reise/aktuell/0,1518,433377,00.html, Stand: 02.10.2009.

141 Vgl. ACTiSYS (2002), S. 1.

142 Vgl. http://www.itwissen.info/definition/lexikon/infrared-financial-messaging-IrFM.html, Stand: 03. 10.2009.

143 Vgl. Durix (2004), S. 3ff.

144 WiFi bezeichnet den Funknetzwerkstandard IEEE802.11b, Vgl. http://www.at-mix.de/wifi.htm, Stand: 02.10.2009.

145 Vgl. Turowski/Pousttchi (2004), S. 54; ACTiSYS (2002), S. 1.

gebetteten Dual-Interface-Chip, bei der alle Daten gemeinsam gespeichert sind und über die Contactless-Schnittstelle gelesen werden können.

Mobiltelefone sind in der Regel mit einer SIM-Karte ausgestattet. Mobile Payment Applikationen funktionieren über die SIM-Karte. Dadurch haben die Mobilfunknetzbetreiber die Möglichkeit, die Zahlungsfunktionalität zu beeinflussen, denn sie können auf alle Daten auf der SIM-Karte zugreifen. Mobiltelefone mit der sog. Dual-Chip-Technik haben zwei Slots, einer für die Telefonie (SIM-Karte) und einer für den Mobile Payment-Chipkarte. Die Banken und Finanzinstitute favorisieren die Dual-Chip-Lösung für die Mobile Payment Transaktionen, da sie dadurch den Mobile Payment Prozess kontrollieren können. Nachteilig ist für die mobilen User, dass sie in die Mobiltelefone mit der Dual-Chip-Ausstattung investieren müssen.[146] Es gab einige Mobile Payment-Pilotprojekte mit der Dual-Chip-Technik, die jedoch nicht erfolgreich waren und nicht länger überlebt haben.[147] Ein Beispiel ist das Pilotprojekt von Nordea mit Nokia und Visa in 2001.[148]

Zusammenfassend kann festgehalten werden, dass die vorgestellten Technologien sowohl für Remote Mobile Payments als auch für Proximity Mobile Payments viele Einsatzmöglichkeiten mitbringen. Jedoch bringen sie auch Risiken und Gefahren für die Sicherheit der Mobile Payment Systeme und den Datenschutz. Die vorgestellten Technologien ermöglichen gleichzeitig auch die kriminellen Umgangsformen wie z. B. der Missbrauch oder die Manipulation der insb. personenbezogenen Daten und Informationen. Beispielsweise ist jeder Datenbesitzer, der über die Daten und Informationen der User verfügt, in der Lage, Kaufverhalten und Lebensstil jedes Users zu analysieren sowie Bewegungsprofile des Users herzustellen und diese mit hoher Wahrscheinlichkeit auch vorauszusagen.[149]

---

146 Vgl. Silberer/ Wohlfahrt/Wilhelm (2002), S. 335.

147 Vgl. Heikkinen (2009), S. 7.

148 Vgl. http://www.visaeurope.com/pressandmedia/newsreleases/press84_pressreleases.jsp, Stand: 19.02.2010.

149 Vgl. Müller-Jung (2010).

2.7 Anwendungsbereiche von Mobile Payments

Mobile Payment findet Anwendung in verschiedenen Lebensbereichen. Je nach Einsatzgebiet unterscheiden sich auch die Anwendungen. Danach werden Mobile Payments in den folgenden Anwendungsbereichen eingesetzt:[150]

- Mobile Content: Mobile Payment für die Abrechnung und Bezahlung digitaler Inhalte und Dienstleistungen
- Mobile Ticketing: Mobile Payment für die Bezahlung von Fahrkarten im öffentlichen Personenverkehr und von Tickets für Veranstaltungen etc.
- Mobile Parking: Mobile Payment für die Abrechnung und Bezahlung von Parkgebühren in Parkplätzen und -häusern
- Mobile Remittance: Mobile Payment Anwendung für die Überweisung von Geldern von z. B. Arbeitsemigranten
- Mobile POS: Mobile Payment für die Bezahlung physischer Güter am POS

Im Folgenden sollen die kurz dargestellten Anwendungsbereiche von Mobile Payments detailliert erläutert werden.

2.7.1 Mobile Content Download

Mobile Content ist eine der Anwendungen des Mobile Commerce und wird als mobil verfügbare, digitale Inhalte des Internets bezeichnet, die mit Hilfe von dargestellten mobilen Technologien angeboten und von mobilen Usern bei Interesse bzw. Bedarf abgerufen, sog. Streaming, bei dem die Audio- oder Videodatei empfangen, jedoch nicht lokal gespeichert werden oder heruntergeladen werden.[151] Mobile Content Produkte oder Dienstleistungen sind jede Art von Medien, die per Mobiltelefon heruntergeladen, auf dem Mobiltelefon angezeigt oder verwendet werden können. Danach können die Mobile Content Produkte und Dienstleistungen in zwei Gruppen unterteilt werden:

---

[150] Vgl. mit den Erläuterungen im Abschnitt 2.4 Mobile Payment Typen, S. 23.

[151] Vgl. mit den Erläuterungen im Abschnitt 2.1 Innovationen und Trends im Bereich „Mobile“, S. 12.

1. Mobile Entertainment: Unter Mobile Entertainment sind alle Formen der Unterhaltung wie z. B. Download und Abspielen der Musikstücke oder Videos etc. zu verstehen, bei denen mobile Endgeräte als Bedien- sowie Übertragungsmedium eingesetzt werden.[152] Das wird auch als Mobile Unterhaltung bezeichnet. Es sind mobile und digitale Inhalte für die Unterhaltung, die mobile User gegen Entgelt abrufen bzw. herunterladen können. In diese Kategorie fallen solche mobilen Inhalte wie Klingeltöne, Musikstücke, TV, Radio, Videos, Spiele etc.[153]

2. Mobile Informationsdienste: Das sind redaktionelle Inhalte von Zeitungs- und Zeitschriftverlagen oder lokalen Informationsdiensten von Städten, Metropolen, Tourismusbehörden. Diese Inhalte oder Dienstleistungen werden auch als Location Based Services bezeichnet.[154] Die Beispiele für die mobilen Informationsdienste sind aktuelle News, Schlagzeilen von Zeitungen, Stadtpläne und Reiseinformationen etc.[155]

Bei Mobile Content Download ist der mobile User nicht anonym, da er seine Mobilfunknummer sowie andere personenbezogenen Daten an den MCP und anderen Marktteilnehmern preisgeben muss. Die meisten Mobile Content Download Portale erfordern eine Registrierung der User, die keine User-Anonymität gewährleisten.[156]

2.7.2 Mobile Ticketing

Das Mobile Ticketing ist eine weitere Anwendung des Mobile Commerce, bei der mobile User mit dem Einsatz vom Mobiltelefon Fahrkarten und Tickets bestellen, bezahlen, erhalten und validieren können. Mobile Ticketing wird gegenwärtig in den folgenden Bereichen verwendet:

---

[152] Vgl. http://www.ccwap.de/m_entertainment.htm, Stand: 07.10.2009.

[153] Vgl. Hess et al. (2005), S. 65ff. sowie http://www.ccwap.de/m_entertainment.htm, Stand: 07.10. 2009.

[154] Vgl. mit den Erläuterungen im Abschnitt 2.1.2 Location Based Services, S. 14.

[155] Vgl. http://www.horizont.net/aktuell/medien/pages/protected/Verlage-setzen-auf-mobile-Informatio nsdienste_63886.html, Stand: 07.10.2009.

[156] Diese Anwendungsform wird als Praxisbeispiel im Abschnitt 6.4 Referenzprozessmodell zur Gestaltung der User-Anonymität in Mobile Payment Systemen, S. 160 näher erläutert.

- im öffentlichen Personennah- und -fernverkehr (ÖPNV), im Bus- und Bahnverkehr, im Schiff- und Flugverkehr.[157] Als Beispiele für Mobile Ticketing im ÖPNV sind das Handy-Ticket (sowie Testprojekt Touch & Travel) der Deutsche Bahn[158] und das RMV-HandyTicket zu nennen.[159]

- bei den sportlichen und kulturellen Veranstaltungen wie Spiele, Events, Museen, Kino und Theater[160]

- Parkplätzen und Parkhäusern[161]

Mit Mobile Ticketing erzielen sowohl User als auch Service Provider Kosten- und Komfortvorteile. Mit dem Einsatz von Mobile Ticketing werden die Einnahmen von Serviceanbietern erhöht. Dabei werden die Kosten der Erstellung und Verteilung von Papiertickets reduziert sowie die Bequemlichkeit (sog. Convenience) von Usern und ihre Zufriedenheit dadurch erhöht. Während das Handyticket im ÖPNV breit genutzt wird, ist das Handyparken noch nicht zum Massenphänomen geworden.[162]

Mobile Tickets werden über verschiedene Wege abgewickelt und mobile User erhalten ihre Tickets auf ihre Mobilfunkgeräte durch die folgenden Techniken[163]:

- Textbasierte Tickets mit SMS-Technik[164]

- Textbasierte Tickets mit WAP Push-Technik[165]

- Bild/Barcode-basierte Tickets mit SMS, EMS[166], MMS-Technik[167]

---

157 Vgl. http://www.bahn.de/p/view/buchung/mobil/handy_ticket.shtml und http://www.dashandyticket.de/index.html sowie Testprojekt Touch& Travel: http://www.touchandtravel.de/site/touchandtravel/de/start.html, Stand: 22.02.2010.

158 Vgl. http://www.bahn.de/p/view/buchung/mobil/handy_ticket.shtml, Stand: 08.10.2009.

159 Vgl. http://www.rmv.de/coremedia/generator/RMV/Tickets/RMVHandyTicket, Stand: 08.10.2009.

160 Vgl. http://www.elegate.de/?id=556, Mobile Ticketing - für "Kurzentschlossene", Stand: 08.10.2009.

161 Vgl. http://www.mobil-parken.de/cms/, Stand: 08.10.2009 sowie mit dem Abschnitt 2.7.3 Mobile Parking, S. 44.

162 Vgl. http://www.heise.de/newsticker/meldung/Anruf-statt-Parkschein-194915.html, Stand: 08.10.2009.

163 Vgl. Mobile Ticketing, http://mobile8u.com/?page_id=276, Stand: 20.02.2010.

164 Vgl. Neuhaus (2003), S. 97ff. sowie o. V. (2007b), S. 3.

165 Vgl. Ebenda.

- Dedicated Mobile Application[168] wie Java Plattform Micro Edition[169]
- RFID-Technik[170]
- Voice[171]

Auch bei Mobile Ticketing muss sich der mobile User bei den Anbietern der Mobile Ticketing Systeme registrieren, damit er die Mobile Ticketing Dienstleistungen nutzen kann. Deshalb bietet Mobile Ticketing keine User-Anonymität. Die hinterlassenen Daten bieten Persönlichkeits- und Bewegungsprofile mobiler User herzustellen.[172]

2.7.3 Mobile Parking

Eine andere Anwendung ist das Mobile Parking, mit dem Parkgebühren in gebührenpflichtigen Parkplätzen und Parkhäusern per Mobiltelefon oder ein anderes Mobilfunkgerät bezahlt werden können. Mobile Parking kann erfolgen:[173]

- per mobilen Anruf an einen Payment Service Provider und/oder

---

166 EMS steht für Enhanced Messaging Service. EMS ist die Erweiterung des SMS-Dienstes und baut auf die SMS-Definition auf. EMS ergänzt das textbasierte SMS um Bilder, Töne und Animationen. Vgl. http://www.computerbase.de/lexikon/Enhanced_Message_Service sowie http://www.elektronik-kompendium.de/sites/kom/0601221.htm, Stand: 31.01.2009.

167 Vgl. Neuhaus (2003), S. 97ff. sowie http://www.messagenet.com.au/PR%5CFRE_MobileTicketing_D03.pdf, S. 3, Stand: 20.02.2010.

168 Vgl. Mobile Ticketing, http://mobile8u.com/?page_id=276, Stand: 20.02.2010.

169 Vgl. http://java.sun.com/javame/index.jsp, Stand: 31.01.2009.

170 Vgl. BSI (2004), S. 23.

171 Dabei werden mobile Zahlungstransaktionen mit der eigenen Stimme (Stimmverifizierungsverfahren) statt TAN- oder PIN-Verfahren autorisiert und freigegeben, z. B. Voice Pay. Vgl. Brinker/Scholz (2007), S. 1ff. sowie http://www.voice-pay.com/index.html, Stand: 24.02.2010.
TAN: Transaktionsnummer, die bei jedem Buchungsvorgang im Rahmen des Electronic Banking eingegeben werden muss. Sie ist eine Ergänzung zur Persönlichen Identifikationsnummer (PIN). Die TAN wird von der Bank als Quasi-Unterschrift interpretiert. Sie verfällt nach einmaligem Gebrauch. Vgl. Brinker/Scholz (2007), S. 7. Es gibt auch verbesserte (indizierte und mobile) Varianten von TAN wie iTAN und mTAN als Schutz gegen Phishing und Trojanische Pferde. Vgl. http://www.postbank.de/itan, Stand: 24.02.2010.

172 Vgl. mit den Erläuterungen im Abschnitt 6.2 Analyse eines allgemeinen Mobile Payment Prozesses, S. 154 sowie im Abschnitt 6.3 Bewertung des allgemeinen Mobile Payment Prozesses hinsichtlich der User-Anonymität, S. 159.

173 Vgl. Ronzheimer (2005), S, 5.

- per mobile Datenübertragung z. B. durch WLAN oder NFC[174]

Beim Mobile Parking per mobilen Anruf sind die Parkzonen mit individuellen Rufnummern gekennzeichnet. Der mobile User wählt diese Rufnummer beim Starten und Beenden jedes Parkvorgangs. Wenn der User auf solchen gekennzeichneten Parkzonen parken möchte, ruft er den Parksystemanbieter an. Daraufhin bekommt er eine SMS-Bestätigung, dass der Parkvorgang beginnt. Der Parksystemanbieter nimmt den User in die Liste der parkenden Fahrzeuge auf. Für das Beenden des Parkvorgangs wählt der User die Rufnummer der Parkzone nochmals an. Der Parksystemanbieter stoppt die Parkuhr und entfernt den User aus der Liste der parkenden Fahrzeuge und rechnet ab und sendet eine SMS-Bestätigung, dass der Parkvorgang beendet ist. Bei einigen Systemen kann der User nur einmal die Parkzonenrufnummer wählen und die Uhrzeit für den Parkbeginn und Parkende nennen. Mobile Parking per mobile Datenübertragung hingegen erfolgt über die Nutzung von mobilen Technologien wie z. B. WLAN oder NFC. Es wird vermutet, dass Parken und Parkgebühren in naher Zukunft über das Navigationsgerät koordiniert und abgerechnet werden.[175]

Mobile Parking bietet folgende Vorteile:[176]

- Zeit-, orts- und bargeldlose Bezahlung von Parkgebühren wird ermöglicht
- Mit dem Mobiltelefon können viele User Mobile Parking nutzen
- Mobile Parking wird minutengenau abgerechnet
- Detaillierte Informationen über die Nutzung von Parkplätzen werden gewonnen

Der Nachteil beim Mobile Parking ergibt sich aus der Registrierungsklausel, dass der User sich beim Parksystemanbieter registrieren und ein Kundenkonto errichten muss.[177] Hierbei muss der User seinen Namen, Adresse, Mobilfunknummer, Bankverbindung, E-Mail-Adresse und das Kennzeichen seines Fahrzeugs benennen. Bezahlung von Mobile Parking erfolgt über Kundenkonto mit Einzugsermächtigung oder

---

[174] Vgl. mit den Erläuterungen im Abschnitt 2.1.4 Near Field Communication Services, S. 16 sowie mit dem Abschnitt 2.6.2.1 Near Field Communication, S. 36.

[175] Vgl. Gottschalk (2008).

[176] Vgl. Initiative D21 (2006), S. 5.

[177] Vgl. Parlak (2009), S. 101ff.

über die monatliche Telefonrechnung.[178] Auch Mobile Parking Systeme ohne Registrierung funktionieren nicht ganz anonym, da für das Parken die Kfz- und Mobilfunknummer übertragen werden muss, um den Parkschein per SMS zu erhalten. Außerdem sind die Standortinformationen des parkenden Users bekannt.

2.7.4 Mobile Remittance

Eine andere Entwicklung ist Mobile Remittance. Diese neue Anwendung erlaubt den mobilen Usern, Geld an andere Konten, Banken und Usern sowohl national als auch international zu senden, in dem sie ihre Mobiltelefone verwenden. Mobile Remittance Service wird häufig von Arbeitsemigranten benutzt und ist für sie ein sehr wichtiger Service, weil sie damit ihre Löhne und Gehälter auf ihre Prepaid-Konten überwiesen bekommen und dann das Geld in ihre Heimatländern senden können.[179] Mobile Remittance erfolgt sowohl vom Mobilfunkgerät zu einem anderen Mobilfunkgerät als auch vom Mobilfunkgerät zu einem Bank- oder Kreditkartenkonto.

Mobile Remittance kann insbesondere in den Märkten von Entwicklungs- und Schwellenländern beobachtet werden. Einige Beispiele hierfür sind die Philippinen und Kenia. Allerdings sind die Transaktionskosten für die grenzüberschreitenden Überweisungen durch die Bankkanäle wegen der fehlenden Standardisierung sehr hoch. In den Ländern Lateinamerikas, Afrikas und teilweise auch Asiens sind Bankinfrastrukturen geografisch wenig verbreitet. Auch sind in dieser Gruppe von Ländern die Transaktionskosten grenzüberschreitender Überweisungen verglichen mit den landesüblichen Kosten hoch. In den Entwicklungs- und Schwellenländern sind mobile Finanzdienstleistungen für eine große Anzahl von Usern die einzige Möglichkeit, Finanzprodukte zu erwerben bzw. Finanzdienstleistungen zu nutzen.[180]

Mobile Remittance in der Praxis können anhand einiger Beispiele aus verschiedenen Weltregionen erklärt werden:

Philippinnen

---

[178] Vgl. mit dem Abschnitt 6.2 Analyse eines allgemeinen Mobile Payment Prozesses, S. 154 sowie dem Abschnitt 6.3 Bewertung des allgemeinen Mobile Payment Prozesses hinsichtlich der User-Anonymität, S. 159.

[179] Eine neue Entwicklung ist aktuell in den Formen der Remittances zu beobachten. Von (Arbeits-) Emigranten werden nicht nur Remittances, also Geldüberweisungen sondern auch Sachüberweisungen in die Heimatländer getätigt. Vgl. Bös (2010).

[180] Vgl. Sam (2009); Krohn (2009).

SMART ist mit ca. 23 Mio. Abonnenten der größte Mobilfunknetzbetreiber auf den Philippinen, bietet u.a. SMS basierte Mobile Remittance Services, bekannt als „SMART Padala“[181]. Mit diesem Service können philippinische Arbeitsemigranten z.B. in Australien, Canada, USA, Spanien, UAE etc. Gelder aus ihren im Ausland verdienten Löhnen und Gehältern in ihr Heimatland zu senden. Der Service sendet eine Textnachricht sowohl an den Empfänger als auch den Sender, dass der Geldbetrag überwiesen wurde. Der Empfänger kann dann diesen Geldbetrag über sein Mobilfunkkonto autorisieren und diesen bei einem Partnerinstitut auf den Philippinen abholen. Der Service Provider belastet bei jeder Remittance-Transaktion das Kundenkonto mit 1 % Transaktionskommission. Zudem wird eine Airtime[182]-Gebühr von 0,04 US Dollar pro Minute berechnet. Insgesamt zahlt der User aber weniger im Vergleich zu den anderen normalen Remittance-Services.[183]

Globe Telecom, ein anderer zweiter Mobilfunknetzbetreiber auf den Philippinen, bietet auch einen ähnlichen Mobile Remittance Service, bekannt als „G-Cash“[184]. Mit diesem Service können philippinische Kleinverdiener und Arbeitsemigranten in den USA, UK, Australien, Taiwan etc. Überweisungen per SMS an den Globe Telecom Abonnenten auf den Philippinen ausführen. Der Empfänger erhält das überwiesene Geld in den Globe Telecom Shops ausgezahlt, indem er sein Mobiltelefon mit der SMS-Nachricht und seinen Personalausweis vorzeigt. Dieser Service kann auch innerhalb der Philippinen benutzt werden. Der Empfänger zahlt an den Serviceanbieter Transaktionsgebühren bis zu 1 % des Überweisungsbetrages. Um diesen Service nutzen zu können, braucht der User sein Mobiltelefon und eine einmalige Registrierung beim Serviceanbieter.[185]

Kenia

Ein anderes Beispiel für die Mobile Remittance ist M-PESA[186], das von Safaricom und Vodafone in einem Joint-Venture betrieben wird. Mit dem M-PESA Service können Mobile User Geldtransfers mit dem Mobiltelefon durchführen. Die User oder

---

[181] Vgl. http://smart.com.ph/Corporate/Services/SmartPadala/, Stand: 28.02.2009.

[182] Airtime bezeichnet die Gesamtzeit der verbrauchten Minuten des Users, die er mit der Nutzung des Mobilfunkgerätes für ankommende und ausgehende Telefonate konsumiert hat. Vgl. MMA (2008), S. 3.

[183] Vgl. Wishart (2006), S. 9ff. sowie http://globaltechforum.eiu.com/index.asp, Stand: 28.02.2009.

[184] Vgl. http://www.g-cash.com.ph/, Stand: 28.02.2009.

[185] Vgl. Wishart (2006), S. 25ff. sowie http://globaltechforum.eiu.com/index.asp, Stand: 28.02.2009.

[186] Vgl. http://www.safaricom.co.ke/index.php?id=745, Stand: 01.03.2009

deren Bekannten, Freunde oder Verwandten können das überwiesene Geld entweder bei M-PESA-Agenten oder bei einer ATM abheben. Für die Nutzung vom M-PESA Service müssen sich die User einmalig in den M-PESA-Agenten in Kenia registrieren und eine M-PESA-Applikation auf den SIM-Karten von Mobilfunkgeräten speichern. Die User brauchen dabei kein Bankkonto zu haben, um den M-PESA-Service nutzen zu können. M-PESA bietet einen sehr hilfreichen Service für die Leute, die auf ländlichen Gebieten wohnen und deshalb schlechte Zugangsmöglichkeiten zu einer Bank haben oder sich kein Bankkonto leisten können. Weil das Geld im Namen von M-PESA auf einem Bankkonto verwaltet wird, gibt es keinen Kontakt zwischen den Usern und der Bank. Detaillierte Userdaten werden im M-PESA gehalten und nicht an die Banken weitergegeben.

Bei Mobile Remittance bleiben weder der Sender noch der Empfänger der Geldüberweisung anonym, da sich der Sender registrieren und der Empfänger in der Mobilfunkfiliale ausweisen muss.

2.7.5 Mobile POS

Die Bezeichnung „Point of Sale“ beschreibt im Allgemeinen die Erfassung von Verkaufsdaten mit Zeit- und Ortsangabe. Die POS-Systeme verwenden Rechner oder spezielle Terminals, die mit Registrierkassen, Strichcode-Lesegeräten, optischen Scannern und Magnetstreifen-Lesegeräten verbunden sind, um die Transaktionen genau und sofort zu erfassen. Die POS-Systeme können entweder zu einem Zentralrechner für Kreditwürdigkeitskontrolle und Inventar-/Bestandskontrolle online verbunden sein oder sie können einzelne PCs sein, die tägliche Transaktionen durchführen und diese speichern, bis diese zu einem Zentralcomputer übertragen werden, der die Transaktionen weiterarbeitet.[187]

Die POS-Terminals bei Händlern sind ein bevorzugter Weg der Verarbeitung von Zahlungstransaktionen mit Kredit- und Debitkarten, Schecks sowie Chipkarten (sog. Smartkarten). Die POS-Terminals bieten vor allem eine geeignete Lösung, sowohl für die Kunden, die nach flexiblen Zahlungsmöglichkeiten beim Einkaufen suchen, als auch für die Händler, die ihre Kosten verringern möchten. Mit den neuen Proximity-Technologien wie z. B. NFC können Mobile Payments am POS für den User flexibler gestaltet werden.[188] Wenn User beim Einkaufen in stationärem Handel

[187] Vgl. o. V. (2010a).

[188] Vgl. mit dem Abschnitt 2.1.4 Near Field Communication Services, S. 16.

bezahlen, geben die Händler zuerst die Zahlungsinformationen ein und dann halten die User ihre Mobiltelefone (ausgerüstet mit einer NFC-Technologie) nahe vor den Terminal. Somit wird eine Verbindung zwischen Terminal und Mobiltelefon hergestellt. Danach wird der mobile User identifiziert und authentifiziert. Die abschließenden Arbeiten der Zahlungstransaktion werden dann vom Terminal durchgeführt. Dann erhält der mobile User einen Kassenbon oder eine Quittung.[189] Es gibt auch Nachteile und offene Fragen mit dem Mobile POS. Der Nachteil, sowohl für User als auch für Händler, sind zusätzliche Kosten, die durch die Anschaffung der Mobilfunkgeräte und Terminals mit der NFC-Technologie und Nutzung der NFC-Services entstehen. Außerdem sollen die Sicherheitsaspekte in Bezug auf personenbezogenen Daten und Information noch geklärt werden. Mobile POS bietet keine User-Anonymität, da der mobile User sowohl seine personenbezogenen Daten als auch seine Aufenthaltsinformationen an die Mobile POS Systeme überträgt.

2.8 Mobile Payment Initiativen

Es gibt auf dem Mobile Payment Markt viele verschiedene Initiativen und Kooperationen wie z. B. Open Mobile Alliance etc. zwischen den Marktteilnehmern, die für die Schaffung neuer und allgemeiner Standards und Technologien im Mobile Payment gegründet wurden. Diese neuen und allgemeinen Standards und Technologien betreffen nicht nur die Mobile Payment Verfahren sondern auch die Sicherheitsfunktionen, wie z. B. die User-Anonymität oder DRM, Kommunikations- und Netzwerktechnologien. Sie spielen deshalb eine entscheidende Rolle bei der Gestaltung der User-Anonymität. Die meisten Initiativen werden von Mobilfunknetzbetreibern, Finanzdienstleistern oder Mobilfunkgeräteherstellern vorangetrieben. Jedoch gibt es unterschiedliche Kooperationsplattformen, die, jeweils von einer Gruppe an Unternehmen initiiert, ähnliche Interessen verfolgen. Aber auch gibt es EU-finanzierte Projekte wie z. B. SEMOPS. Im Folgenden werden die sechs wichtigsten Mobile Payment Initiativen erläutert:

- Open Mobile Alliance (OMA) und Open Handset Alliance (OHA) sind Kooperationen der vielen in der Mobilfunkindustrie tätigen Unternehmen entlang der gesamten Wertschöpfungskette.

[189] Vgl. o. V. (2010a).

- Mobile Payment Forum (Mobey Forum) ist eine Kooperation zwischen den Finanzdienstleistern und Mobilfunkgeräteherstellern.
- Open Mobile Terminal Platform (OMTP) ist eine Kooperation zwischen Mobilfunknetzbetreibern und Mobilfunkgeräteherstellern.
- Secure Mobile Payment Service (SEMOPS) ist eine von der EU finanzierte Projektinitiative für die Entwicklung eines Electronic Payment Systems.
- Pay Buy Mobile ist eine Initiative von GSMA (Global System for Mobile Communications Assosiation).

2.8.1 Open Mobile Alliance

Die Open Mobile Alliance (OMA) ist mit Sitz in Kalifornien in den Vereinigten Staaten im Juni 2002 aus einer Initiative von einigen auf dem mobilen Informations- und Kommunikationsmarkt tätigen Unternehmen wie z. B. Ericsson, Siemens, Nokia, Sony Ericsson, Samsung und Telefónica, Vodafone, Orange, T-Mobile sowie Microsoft, Sun Microsystems, IBM, Oracle etc. gegründet worden.[190] Sie ist eine Standardisierungsorganisation mit dem Ziel, weltweit offene und einheitliche Standards für die im Internet verfügbaren Services und Applikationen für Mobilfunkgeräte zu definieren und zu entwickeln.[191] OMA hat derzeit ca. 400 Mitglieder aus der gesamten Wertschöpfungskette der Mobilfunkindustrie unter anderem Mobilfunknetzbetreiber, Mobilfunkendgeräte- und Netzwerkanbieter, Informationstechnologieunternehmen, Applikationsanbieter, Service und Content Provider.

Die OMA konzentriert sich auf die Entwicklung von marktorientierten, interoperablen Mobilfunk-Service-Enablers für die zusammenwachsende mobile Kommunikation, Unterhaltung und Medien. Einige wichtige Beispiele für solche Enablers sind WAP-Browser-Spezifikationen, MMS-Spezifikationen, DRM-Spezifikationen für Digitale Rechte Management sowie IMPS-Spezifikationen für Instant Messaging[192] auf Mobil-

---

190 Vgl. http://www.openmobilealliance.org/AboutOMA/Default.aspx, Stand: 22.02.2010.

191 Vgl. http://www.openmobilealliance.org/AboutOMA/FAQ.aspx, Stand: 22.03.2009.

192 Instant Messaging heißt soviel wie "sofortige Nachrichtenübermittlung". Dem Chatten im Webchat ähnlich, ermöglicht Instant Messaging, nahezu in Echtzeit Nachrichten zwischen den Teilnehmern auszutauschen. Dazu muss ein spezielles Programm, z. B. der Instant Messenger, installiert werden. Er zeigt dem Nutzer u. a. an, welche seiner Freunde ebenfalls zur gleichen Zeit online sind. … Abgesehen von reinen Textnachrichten bieten die meisten Messenger noch zusätzliche

Fortsetzung auf der nächsten Seite

telefonen etc. Die OMA arbeitet auch oft mit den anderen Standardisierungsorganisationen wie 3GPP[193], 3GPP2[194], IETF[195], W3C[196] zusammen, um Überlappungen in der Entwicklung von Spezifikationen zu vermeiden. Es gibt jedoch Kritik und Bedenken bezüglich der DRM-Spezifikationen, da sie nicht userfreundlich sind und keine User-Anonymität erlauben.[197]

2.8.2 Open Handset Alliance

Die Open Handset Alliance (OHA) ist eine Allianz von 47 Technologie- und Mobilfunkgeräteherstellern, um Innovationen im Bereich mobiler Technologien zu fördern und den Usern hochwertige, preiswerte und bessere Produkte anzubieten. Die OHA wurde am 5. November 2007 gegründet. Die OHA besteht aus Mitgliedern von Mobilfunknetzbetreibern, Mobilfunkgeräteherstellern, Halbleiterproduzenten, Softwareunternehmen etc. und wird von Google geführt.[198]

Die Mitglieder der OHA haben gemeinsam das Betriebsystem Android für Mobilfunkgeräte entwickelt, die gegen andere mobilen Betriebssysteme von Apple Inc., Microsoft, Nokia, Palm, Research In Motion und Symbian konkurriert.[199] Alle Mitglieder setzen sich dafür ein, dass das Betriebsystem Android und die Mobilfunkgeräte sowie Dienstleistungen, die dieses Betriebssystem nutzen, einen kommerziellen Erfolg erzielen. Das ist unter der Open Source Lizenz Apache v2 veröffentlicht. Mobilfunkgerätehersteller und Mobilfunknetzbetreiber arbeiten daran, Mobilfunkgeräte, die auf dieser Plattform basieren, zu entwickeln.[200] Datenschützer kritisieren jedoch das Betriebssystem Android aufgrund der Behandlung der persönlichen Daten. Sie unterstellen, dass Google damit auf persönliche Daten zugreift.[201]

Funktionen, wie Dateitransfer, Voice- und Videochats, Grußkarten, SMS-Versand (kostenpflichtig) oder kleine Online-Spiele, die mit anderen Nutzern gespielt werden können. Vgl. http://www.internet-abc.de/eltern/chatten-instant-messaging.php, Stand: 18.04.2009.

193 Vgl. http://www.3gpp.org/, Stand: 18.04.2009.

194 Vgl. http://www.3gpp2.org/, Stand: 18.04.2009.

195 Vgl. http://www.ietf.org/, Stand: 18.04.2009.

196 Vgl. http://www.w3.org/, Stand: 18.04.2009.

197 Vgl. Emmert (2006); Borchers (2003).

198 Vgl. http://www.openhandsetalliance.com/index.html, Stand: 28.03.2009.

199 Vgl. Martellaro (2010).

200 Vgl. Ebenda.

201 Vgl. Hesselbach (2009).

2.8.3 Mobile Payment Forum

Das Mobile Payment Forum ist eine globale Non-Profit-Organisation von Unternehmen aus den Bereichen Finanzdienstleistungen und Mobile Kommunikationstechnologien. Sie wurde im Mai 2000 von weltweit führenden Finanzinstituten und Hersteller mobiler Endgeräte gegründet. Derzeit hat das Mobile Payment Forum 51 Vollmitglieder und Partner. Das Forum wird hauptsächlich von Finanz- und Kreditinstituten geführt und hat das Ziel, mobile Finanzdienstleistungen durch Banken anzubieten. Um dieses Ziel zu erreichen, führt das Mobile Payment Forum die branchenübergreifende Kollaboration, Geschäftsmodellanalyse, Erfahrungsaustausch, Experimente, Kooperation und Kommunikation mit relevanten, externen Stakeholdern. Daher fördert das Mobile Payment Forum sichere und benutzerfreundliche Mobile Banking und Payment Services.[202] Die User-Anonymität ist in ihren Vereinbarungen nicht explizit genannt, lediglich der Umgang mit den persönlichen Daten in Mobile Banking und Payment Services erwähnt, dass sie nicht an die unbeteiligten Dritten weitergegeben werden.[203]

2.8.4 Open Mobile Terminal Platform

Open Mobile Terminal Platform (OMTP)[204] ist ein Forum, das im Juni 2004 auf der Initiative von acht führenden Mobilfunknetzbetreibern, mmo2[205], NTT DoCoMo, Orange, SMART Communications, Telefónica Móviles, TIM (Telecom Italia Mobile), T-Mobile und Vodafone und mehreren Mobilfunkgeräteherstellern wie Nokia, Sony Ericsson und Motorola etc. gegründet wurde.[206]

Das Ziel des OMTP-Forums ist die Festlegung der Anforderungen für mobile Endgeräte auf einer Bedienerplattform, damit standardisierte Anwendungen zur Verfügung gestellt werden können. Durch diese Anwendungen soll den Usern eine einheitliche, vereinfachte und geräteunabhängige Bedienung ermöglicht werden. Dabei soll die Sicherheit von Mobilfunkgeräten verbessert werden. Die OMTP-Initiative

---

202 Vgl. http://www.mobeyforum.org/?page=mobey-in-brief, Stand: 27.03.2009.

203 Vgl. Mobey Forum (2003), S. 7ff.

204 Vgl. http://www.omtp.org/About.aspx, Stand: 28.03.2009.

205 Heute ist mmo2 durch mehrere Übernahmen bzw. Umstrukturierungen unter dem Namen Telefónica O2 Germany bekannt. Vgl. http://www.de.o2.com/ext/portal/online/2096/index, Stand: 29.03.2009.

206 Vgl. http://www.omtp.org/Membership.aspx, Stand: 22.02.2010.

möchte diese Ziele durch die Definition gemeinsamer Standards erreichen. Durch diese gemeinsamen Standards soll ein offenes Rahmenwerk für die Mobilfunkgeräte-hersteller und Software- und Hardwarehersteller geschaffen werden, um OMTP-kompatible Produkte entwickeln zu können.[207]

Obwohl das Forum anfänglich von Mobilfunknetzbetreibern geführt wurde, wächst es entlang der mobilen Wertschöpfungskette als Ganzes und hat inzwischen 35 Mitglieder und Sponsoren. Dadurch ist neben den Mobilfunknetzbetreibern die komplette mobile Wertschöpfungskette mit Mobilfunkgeräteherstellern, Chipherstellern, Content Providern, Software- und Betriebssystementwicklern vertreten und durch eine Gruppe von verschiedenen Unternehmen als Ratgeber unterstützt.[208]

2.8.5 Pay Buy Mobile

Pay Buy Mobile ist eine Initiative von GSMA (Global System for Mobile Communications Assosiation)[209], die in 2007 von führenden Mobilfunknetzbetreibern und u. a. gegründet wurde.[210] Das ist eine globale Mobile Payment Lösung mit der Nutzung von NFC-Technologien, die von zwölf Mobilfunknetzbetreibern in Australien, Frankreich, Irland, Korea, Malaysia, Norwegen, den Philippinen, Singapur, Taiwan, der Türkei und in den Vereinigten Staaten praktisch getestet wird. Damit sollen User mit ihren Mobilfunkgeräten ausgerüstet mit NFC-Technologie Waren und Services im Einzelhandel, Restaurants und Bahnhöfen etc. schnell, einfach und sicher zu bezahlen.[211] Die Pay-Buy-Mobile Initiative baut auf der Infrastruktur der führenden Kreditkartenunternehmen auf, die ihrerseits Spezifikationen entwickelt haben, um eine weltweite Kompatibilität zwischen Contactless-Chipkarten und Kassenterminals zu gewährleisten.[212]

---

[207] Vgl. http://www.teltarif.de/arch/2004/kw26/s14101.html, Stand: 29.03.2009.

[208] Vgl. http://www.omtp.org/Membership.aspx, Stand: 29.03.2009.

[209] Die GSMA ist eine Organisation, die weltweit die Interessen der mobilen Kommunikationsindustrie vertritt. In der GSM Association sind derzeit rund 800 GSM-Mobilfunkanbieter weltweit in 219 Ländern organisiert. Dazu kommen mehr als 200 Unternehmern im Mobile Ökosystem wie z. B. die Hersteller von Netzwerkinfrastruktur und Mobiltelefonen. Vgl. http://www.gsmworld.com/about-us/index.htm, Stand, 22.02.2010.

[210] Vgl. http://www.gsmworld.com/our-work/mobile_lifestyle/mobile_money/index.htm, Stand: 22.02. 2010.

[211] Vgl. Butcher (2008); Scheible (2007).

[212] Vgl. Ebenda.

2.8.6 Secure Mobile Payment Service

Secure Mobile Payment Service (SEMOPS) ist ein von der EU finanziertes Projekt für die Entwicklung eines sicheren, universellen Electronic Payment Services für alle Typen mobiler Zahlungstransaktionen sowie Internet- und POS-Zahlungstransaktionen in der Echtzeit.[213] Das Konzept von SEMOPS berücksichtigt sowohl den regulatorischen Rahmen der EU als auch die Vertrauensaspekte wie Anonymität und Sicherheit in Mobile Payment Systemen.[214]

[213] Vgl. SEMOPS (2008).

[214] Vgl. Pleil (2003); SEMOPS (2008), S. 4; SEMOPS II, http://www.uni-augsburg.de/en/forschungsportal/fak/wiwi/2007/semops.html, Stand: 06.02.2010.

3 Analyse des Mobile Payment Ökosystems

Das Ökosystem von Mobile Payments besteht aus verschiedenen Personen, Unternehmen, Institutionen, Kooperationen sowie Technologien und Anwendungen, die in einer komplexen Beziehung zueinander stehen. In der Abbildung 8, S. 56 wird das Ökosystem von Mobile Payments dargestellt. Bisher wurden die Technologien, Anwendungsbereiche und Initiativen von Mobile Payments erläutert. In diesem Kapitel erfolgt nun eine Analyse, in der die einzelnen Teilnehmer sowie deren Rollen und Interessen im Lichte bisheriger Erläuterungen des Mobile Payment Ökosystems erklärt werden.

Jeder Teilnehmer hat seine eigenen Interessen und stellt seine eigenen Anforderungen gegenüber den anderen Teilnehmern im Mobile Payment Ökosystem. Die Beziehungen zwischen den Teilnehmern hängen von den jeweilig eingesetzten Technologien und Anwendungen sowie den Interessen der Teilnehmer ab. Deshalb sollen im Folgenden zunächst die einzelnen Teilnehmer und deren Rollen in Mobile Payment Ökosystem erläutert werden. Danach werden die Interessen und Anforderungen der einzelnen Teilnehmer erklärt.

3.1 Teilnehmer und Rollen im Mobile Payment Ökosystem

Wie in der Abbildung 8, S. 56 dargestellt wird, befinden sich im Mobile Payment Ökosystem die folgenden Teilnehmer, die beim Zustandekommen von Mobile Payment unterschiedliche Rollen spielen:

- Mobile User
- Händler
- Mobile Content Provider
- Mobilfunknetzbetreiber
- Banken
- Payment Service Provider
- Trusted Third Parties (vertrauenswürdige Dritte oder Vertrauensinstanzen)
- Der Staat bzw. Regulierungsbehörde
- Mobilfunkgerätehersteller

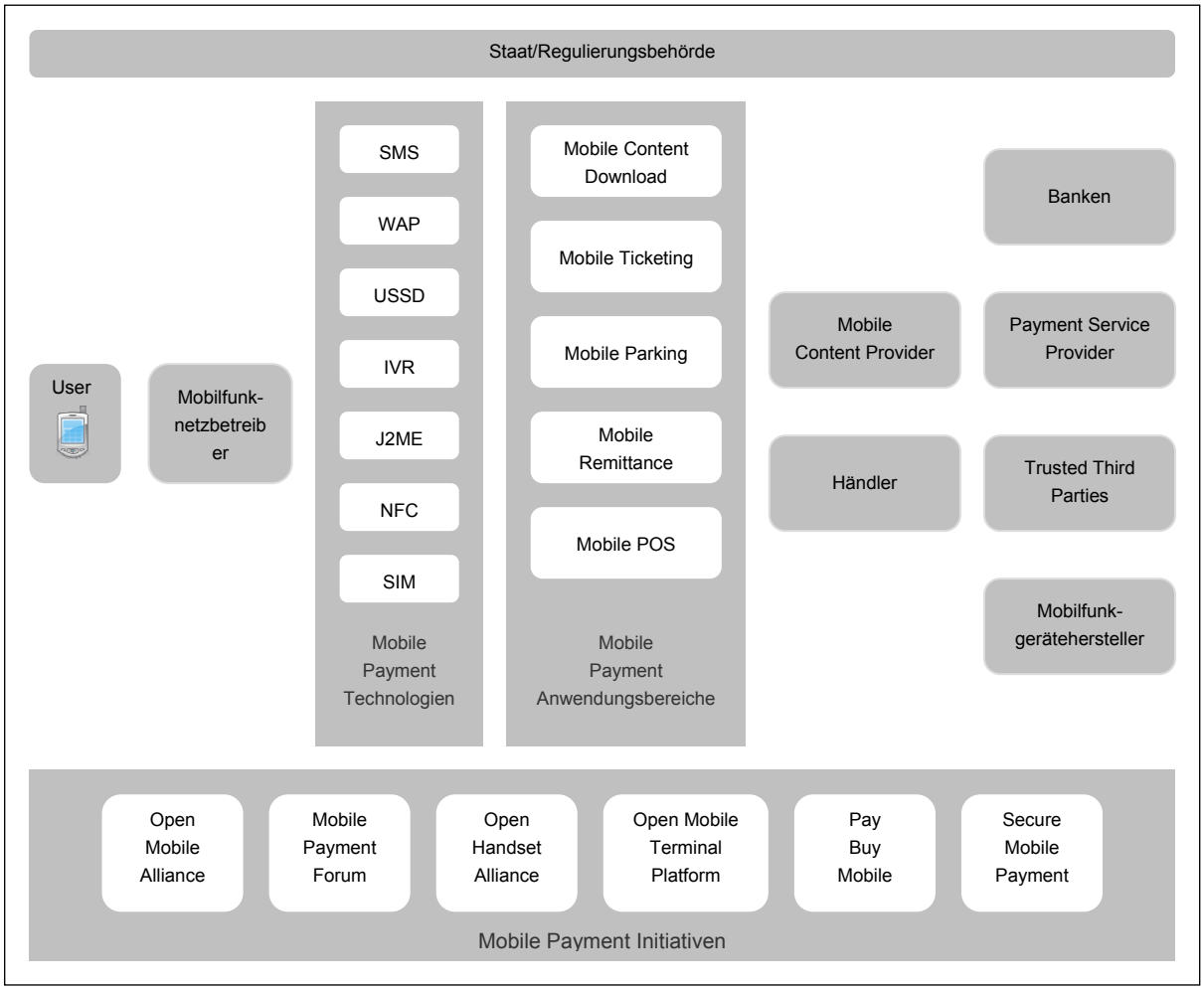

Abbildung 8: Das Ökosystem von Mobile Payments[215]

Im Folgenden werden die einzelnen Marktteilnehmer und deren Rollen im Mobile Payment Ökosystem erläutert.

3.1.1 Mobile User

Mobiler User ist die Person, die ein Mobilfunkgerät besitzt und bereit ist, damit Produkte oder Dienstleistungen zu erwerben bzw. zu bezahlen. Bei den Produkten oder Dienstleistungen, die ein mobiler User kauft, handelt es sich um physische Produkte oder digitale bzw. nicht-digitale Dienstleistungen.[216] Die Rolle mobiler User

[215] Die Abbildung beschränkt sich auf die wichtigen Elemente, also die Hauptteilnehmer, Initiativen, Technologien und Anwendungen, die in dieser Dissertation erwähnt werden.

[216] Die Beispiele für die physische Produkte sowie digitalen bzw. nicht-digitalen Dienstleistungen werden im Abschnitt 2.7 Anwendungsbereiche von Mobile Payments, S. 41 ausführlich erläutert.

beinhaltet die Initiierung mobilen Einkaufs, falls nötig zuerst die Registrierung beim Payment Service Provider und die Autorisierung der Zahlung.

Mobile User stellen die größte Teilnehmergruppe im Mobile Payment dar. Deshalb verdient ihre Stellung besondere Beachtung, denn sie sind die Hauptabnehmer von Mobile Payment Services. Die Erwartungen mobiler User sind vielfältig. Die anderen Marktteilnehmer sollen diese Erwartungen gut kennen und erfüllen. Die Kunden erwarten mit den Mobile Payments einen persönlichen Service mit minimalem Aufwand und Lerneinsatz. Sie möchten sichere und vertrauenswürdige Services und Lösungen sowohl auf technischer als auch auf sozialer Ebene, da mobile User in verschiedenen Situationen (z. B. Urlaub, Reisen, Parken und Einkaufen in der Stadt und Veranstaltungen etc.)[217] einkaufen und bezahlen.[218]

3.1.2 Händler

Händler - sowohl stationär als auch online - sind Einzelpersonen oder Unternehmen, die Produkte und Dienstleistungen an den mobilen User anbieten bzw. verkaufen. Die Rolle der Händler im Mobile Payment ist die Bereithaltung weit verbreiteter Zahlungsmöglichkeiten für die mobilen User. Dabei beinhaltet die Rolle der Händler die Weiterleitung der Kaufanfragen an den Payment Service Provider, die Übermittlung der Autorisierungsanfragen an die User und die Lieferung der Produkte oder Dienstleistungen. Der Händler braucht in der Regel personenbezogene Daten vom User, um das gekaufte Produkt oder die Dienstleistung an diesen zu liefern. Der Händler braucht z. B. die Lieferadresse für die Lieferung an den Empfänger der Leistung und die Bankverbindung für den Geldtransfer. Der Händler sendet personenbezogene Daten und Transaktionsdaten an den Payment Service Provider und die Trusted Third Party (TTP, Vertrauensinstanz), damit die Zahlungstransaktion durchgeführt werden kann.[219]

---

[217] Vgl. mit den Erläuterungen im Abschnitt 2.7 Anwendungsbereiche von Mobile Payments, S. 41.

[218] Die Interessen und Anforderungen der User werden im Abschnitt 3.2.4.1 Anforderungen der mobilen User, S. 72 näher erläutert.

[219] Die Interessen und Anforderungen der Händler werden im Abschnitt 3.2.4.2 Anforderungen der Händler, S. 75 näher erklärt.

3.1.3 Mobilfunknetzbetreiber

Mobilfunknetzbetreiber, auch Mobile Network Operator (MNO) genannt, sind die Betreiber von mobilen Telekommunikationsnetzwerken und spielen eine besondere Rolle im Mobile Payment, da sie als Mobilfunknetzbetreiber eine technische Infrastruktur und als Telekommunikationsanbieter mobile Telekommunikationsdienste anbieten. Mobilfunknetzbetreiber können ihre bestehenden Abrechnungssysteme für das Mobile Payment nutzen.[220] Neben den Banken haben Mobilfunknetzbetreiber einen direkten Zugang zu einer breiten Kundenbasis, um Mobile Payment Services anzubieten. Mobilfunknetzbetreiber besitzen eine kritische Position in Mobile Payment Systemen, da die Zahlungstransaktionen über die Mobilfunknetzbetreiber durchgeführt werden und Mobilfunknetzbetreiber einen Zugriff zu den personenbezogenen Daten sowie Verbindungs- und Transaktionsdaten mobiler User haben.[221] Diese können sie für verschiedene Marketingmaßnahmen nutzen und mobile User gezielt ansprechen. Aus diesem Grund sind Mobilfunknetzbetreiber in einer besonderen und wichtigen Vertrauenspflicht gegenüber dem User.[222]

3.1.4 Banken

Banken haben eine wichtige Rolle im Zahlungsverkehr und möchten diese Rolle auch im Bereich Mobile Payment beibehalten. Banken sind genauso wie Mobilfunknetzbetreiber in einer besonderen Vertrauenspflicht. Bei einer mobilen Zahlungstransaktion übernehmen Banken sowohl die Rolle eines Finanzdienstleisters als auch die Rolle einer TTP als Vertrauensinstanz. Banken brauchen personenbezogene Daten des Users und Transaktionsdaten, um die Zahlungstransaktionen zwischen den Usern und Händlern durchzuführen. Banken erhalten diese Daten in der Regel vom Händler. Banken und Kreditinstitute haben großes Interesse an Mobile Payment Systemen, da sie dadurch neue Geschäftsfelder und Ertragsquellen erschließen möchten. Dabei möchten Banken ihre Kompetenzen erweitern und ihre

---

[220] Vgl. Zhou/Bergmann/Schlang (2004), S. 30.

[221] Vgl. Ebenda, S. 30 und 53; Henkel (2002), S. 341.

[222] Die Interessen und Anforderungen der Mobilfunknetzbetreiber werden im Abschnitt 3.2.4.3 Anforderungen anderer Marktteilnehmer, S. 77 näher erörtert.

Marktposition im Wettbewerb stärken.[223] Jedoch können Banken diese Kundenbasis und ihre Daten für ihre Zwecke nutzen.[224]

3.1.5 Mobile Content Provider

Der Gesetzgeber definiert einen Content Provider in § 2 Absatz 1 vom Telemediengesetz als „*Diensteanbieter jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt.*“ [225] Danach ist ein Content Provider ein Serviceunternehmen, das eigene oder fremde Inhalte digitaler Art zur Nutzung durch die Dritten anbietet. Diese Inhalte können personalisierter, zielgruppenspezifischer und digitaler Art sein.

Die Content Provider bieten für die mobilen Enduser gebündelte Dienste wie News, Wetterdienste, Börsenkurse, Suchmaschinen, Maildienste, Maps, Routenplaner, Fahr- und Flugpläne, Musikdownload, Spiele und Unterhaltung etc. Darüber hinaus bieten MCP, die auf dem Gebiet der Bereitstellung mobiler Inhalte spezialisiert sind, digitale Inhalte wie Mobile News, Mobile Transport Information, Mobile Financial Information Services, Mobile Music, Mobile Game, Mobile Film und Video etc. für das Mobiltelefon an.[226]

Der Content Provider kann die digitalen Inhalte über das Internet oder Intranet anbieten. Die Inhalte über das Internet werden kostenpflichtig oder kostenfrei angeboten, während die Inhalte über das Intranet nur für die zugangsberechtigten Mitarbeiter eines Unternehmens angeboten werden. Content Provider können spezialisierte Firmen, Online-Dienste, private Personen, Behörden, Vereine oder Bildungseinrichtungen sein.[227]

3.1.6 Mobile Payment Service Provider

Payment Service Provider sind für die Zahlungsabwicklung verantwortlich und steuern den Prozess der Buchung zwischen den mobilen Usern, den Händlern bzw.

---

223 Vgl. Zhou/Bergmann/Schlang (2004), S. 29ff.

224 Die Interessen und Anforderungen der Banken und Kreditinstitute werden im Abschnitt 3.2.4.3 Anforderungen anderer Marktteilnehmer, S. 77 näher behandelt.

225 Vgl. http://www.gesetze-im-internet.de/tmg/__2.html, Stand: 11.10.2009.

226 Vgl. European Communities (2002), S. 4ff.

227 Vgl. http://www.itwissen.info/definition/lexikon/content-provider-Inhalte-Anbieter-CP.html, Stand: 11.10.2009.

Content Providern und den Trusted Third Parties (Vertrauensinstanzen). Der mobile User muss sich (falls erforderlich) bei einem Payment Service Provider anmelden, um z. B. auf dem Mobilfunkgerät die Wiederholung der Eingabe der Zahlungstransaktionsinformationen zu vermeiden. Beispiele hierfür sind die Kreditkartendaten oder Post-paid-Account-Informationen. Mobile Payment Service Provider (MPSP) können Mobilfunknetzbetreiber, Banken und Kreditkartengesellschaften oder ein unabhängiger Payment Service Provider sein.

MPSP bieten sowohl Händlern als auch Usern Mobile Payment Services an. Mobile Payment Services werden durch Lastschriftverfahren, Banküberweisung oder Online-Überweisung, Kreditkartenbelastungen sowie durch die Payment Service Provider wie PayPal, ClickandBuy etc. abgewickelt. MPSP verbinden verschiedene Mobile Payment Services auf einer Plattform und bieten einen Gesamtservice aus einer Hand (Full-Payment-Service) für die Händler im M-Commerce, der neben der Abwicklung der elektronischen Zahlungstransaktionen auch verschiedene Funktionen wie Risikomanagement, Payment Transaction Matching, Betrugsschutz, Reporting und Multiple Währungen beinhaltet. Mit dem Full-Payment-Service können Payment Service Provider somit den ganzen Payment-Prozess vollständig verwalten. Dadurch sind die Händler weniger von den Kreditinstituten und Banken abhängig, da eine direkte technische Anbindung von Händlern an ein Payment System meistens mit großem Aufwand möglich ist.

3.1.7 Trusted Third Party

Als Trusted Third Party (TTP), auch als Trust Center wird eine Vertrauensinstanz oder vertrauenswürdige Drittinstanz bezeichnet, die hauptsächlich zwei Funktionen in der digitalen Kommunikation erfüllt.[228] Zunächst stellt sie sicher, dass eine Manipulation der übertragenen Daten durch Unberechtigte nicht möglich ist. Zudem stellt sie eindeutig fest, dass die übertragenen Daten tatsächlich von einem berechtigten Absender stammen.[229] Trusted Third Party bzw. Trust Center sind Anbieter von Zertifizierungsdiensten, die im Rahmen einer „Public Key Infrastructure“ für elektronische Signaturen nach dem Signaturgesetz viele wichtige Aufgaben über-

[228] Vgl. Wislsperger (1998).

[229] Vgl. Ebenda.

nehmen.[230] Das sind staatliche oder privatwirtschaftliche Organisationen und Unternehmen. Trusted Third Parties haben verschiedene Aufgaben wie Schlüsselgenerierung, Zertifizierung des öffentlichen Schlüssels, Bereitstellung der Zertifikate (Verzeichnisdienst), Entgegennahme und Ausführung von Sperrungen durch das Trustcenter (Sperrdienst), die amtliche Zeitangabe (Zeitstempeldienst) etc.[231] Die TTP liefern digitale Zertifikate und bestätigen die Identität des Kommunikations- oder Geschäftpartners in digitalen Kommunikationsprozessen. Sie zertifizieren die elektronischen Signaturen bei der elektronischen Übertragung der Daten. Somit ermöglichen sie eine sichere und rechtsverbindliche Signierung elektronischer Daten und Informationen.

Derzeit gibt es zwei Verschlüsselungsverfahren, um eine sichere Kommunikation bzw. sichere Übermittlung vertraulicher Daten zwischen zwei Kommunikationspartner zu gewährleisten.[232] Das erste Verfahren ist das symmetrische Verschlüsselungsverfahren, bei dem derselbe geheime Schlüssel zum Ver- und Entschlüsseln der Daten benutzt wird, der wiederum sowohl Sender als auch Empfänger bekannt sein muss. Das zweite Verfahren ist das asymmetrische Verfahren, das auch „Public Key Infrastructure“ genannt wird. Im Gegensatz zum symmetrischen Verfahren werden für die Ver- und Entschlüssen zwei unterschiedliche Schlüssel, ein privater Schlüssel (Private Key) und ein öffentlicher Schlüssel (Public Key) benutzt. Beim asymmetrischen Verfahren bzw. Public Key Infrastructure werden Nachrichten mit dem öffentlichen Schlüssel verschlüsselt. Diese Nachrichten können dann nur mit dem Privaten Schlüssels entschlüsselt werden. TTPs kommen im asymmetrischen Verfahren (Public Key Infrastructure) zum Einsatz und übernehmen dabei die oben genannten Aufgaben wie Schlüsselgenerierung, Zertifizierung etc. Bei der Nutzung einer Smart-Card wird der geheime Privatschlüssel auf der Karte selbst gespeichert und gleichzeitig der öffentliche Schlüssel bei der TTP hinterlegt.[233] Wenn die Smart-Card zum Einsatz kommt, wird diese mit Hilfe des Privatschlüssels authentisiert.

In TTP-Modellen verwenden alle Parteien dieses Vertrauen durch die TTPs, um ihre eigenen Aktivitäten zu schützen. TTPs werden in kommerziellen Transaktionen, in

---

230 Vgl. Gesetz über Rahmenbedingungen für elektronische Signaturen, http://bundesrecht.juris.de/sigg_2001/BJNR087610001.html#BJNR087610001BJNG000300000 sowie http://www.zertificon.com/trustcenter.php, Stand: 25.02.2010.

231 Vgl. Ebenda; Fox/Horster/Kraaibeek (1995), S. 2ff.

232 Vgl. Binder (2005), S. 5ff.

233 Vgl. http://www.at-mix.de/trust_center.htm, Stand: 12.10.2009.

kryptografischen digitalen Transaktionen beliebig eingesetzt. In der Praxis existieren die sog. Zertifizierungsstellen, auch Certification Authority (CA) genannt, die die Identität der Kommunikationspartner zertifizieren. Die TTPs werden von der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen zugelassen. Für die TTPs gelten strenge Sicherheitsregeln.[234] Prominente Beispiele für TTP bzw. CA sind VeriSign, Thawte und Comodo sowie TC TrustCenter, TeleSec der Deutschen Telekom, Signtrust der Deutschen Post etc.[235]

3.1.8 Staat

Die Rolle des Staates bzw. der Regulierungsbehörden besteht in der Gestaltung neuer Regelungen und Rahmenbedingungen, die eine günstige Grundlage für die Nutzung von Mobile Payments bewirken. Daneben beaufsichtigt der Staat die Gesetzesmäßigkeit der Aktivitäten der Marktteilnehmer im Sinne des allgemeinen Interesses. Daher hat der Staat im Rahmen seiner Rolle innerhalb des Mobile Payment Systems ein großes Interesse an der Prävention und Schutz gegen kriminellen Missbrauch und Geldwäsche.[236] Beispielswiese könnte Mobile Payment als Instrument zur Geldwäsche dienen.[237] Darüber hinaus könnte auch die Anonymität von Mobile Payment das Risiko der Wirtschaftskriminalität erhöhen, da die Anonymität für die User eine ambivalente Eigenschaft mit sich bringt.[238]

3.1.9 Mobilfunkgerätehersteller

Mobilfunkgerätehersteller spielen eine wichtige Rolle im Mobile Payment, da sie mit mobilen Technologien, also den Fähigkeiten der Endgeräte und damit den mobilen Markt erheblich mitbestimmen. Mit Mobile Payment Services haben Mobilfunkgerätehersteller die Möglichkeit, ihre Endgeräte mit neuen eingebetteten Hardware- und Software-Eigenschaften (z. B. NFC, RFID, Mobilebrowser etc.) auf einem breiten Markt einzuführen. Diese entwickeln sie entweder im Alleingang (Proprietäre Standards) oder bilden mit den anderen Herstellern und Partnern wie Telekommunikationsunternehmen, Banken und Applikationsanbieter strategische

---

234 Vgl. http://www.at-mix.de/trust_center.htm, Stand: 12.10.2009.

235 Vgl. http://www.sslshopper.com/certificate-authority-reviews.html, Stand: 12.10.2009.

236 Die Interessen und Anforderungen des Staates werden im Abschnitt 3.2.4.3 Anforderungen anderer Marktteilnehmer, S. 77 näher erläutert.

237 Vgl. Cuche 2001, S. 52.

238 Vgl. Ebenda.

Partnerschaften und Kooperationen, um kompatible, weit verbreitete Standards und multifunktionale Endgeräte und Applikationen im Alleingang oder in verschiedenen Initiativen. [239] Damit haben Mobilfunkgerätehersteller das Ziel, die Kosten der Entwicklung und Integration von neuen Technologien zu senken. Die Gerätehersteller erwarten damit kurze Produkteinführungszeiten und hohe Absatzzahlen von mobilen Endgeräten wie Handys und Smartphones.

3.2 Interessen und Anforderungen der Marktteilnehmer

Eine wichtige Voraussetzung für die Akzeptanz der Mobile Payments ist die Berücksichtigung der Interessen und Anforderungen aller Marktteilnehmer im Mobile Payment Ökosystem. Die Interessen von Marktteilnehmern können durch deren Ziele im Mobile Payment Ökosystem formuliert werden und sind jedoch recht unterschiedlich. Die Anforderungen an Mobile Payment hingegen ergeben sich aus den Wünschen, Erwartungen und Bedürfnissen von Marktteilnehmern. Wie in der Abbildung 9, S. 64 dargestellt wird, können die Anforderungen in vier Gruppen unterteilt werden.

Bei den Anforderungen werden zunächst allgemeine, technische, funktionale und wirtschaftliche sowie benutzerspezifische Anforderungen unterschieden[240], die im Folgenden ausführlich erläutert werden.

3.2.1 Allgemeine Anforderungen

Die Marktteilnehmer stellen folgende allgemeine Anforderungen an Electronic Payment Systeme.[241] Diese Anforderungen können mit den Anforderungen an Mobile Payment Systemen ergänzt werden, die sich aus der Mobilität und Interaktion der User mit der mobilen Umgebung resultieren. Die Folgen der Mobilität und Interaktion der User für die mobilen Geschäftsprozesse und mobilen Transaktionen im M-Commerce müssen ebenfalls berücksichtigt werden.

Die allgemeinen Anforderungen können wie folgt dargestellt werden:

---

[239] Vgl. mit den Erläuterungen im Abschnitt 2.8 Mobile Payment Initiativen, S. 49.

[240] Vgl. Himmelspach et al. (1996), S. 1; Illik (2002), 178ff.

[241] Vgl. Henkel (2001), S. 106.

- **Atomicy (Totalität)** bedeutet, dass eine mobile Zahlungstransaktion vollständig durchgeführt werden kann.

- **Consistency (Konsistenz)** besagt, dass die Integrität der Daten mobiler Zahlungstransaktionen der Marktteilnehmer gewährleistet werden muss.

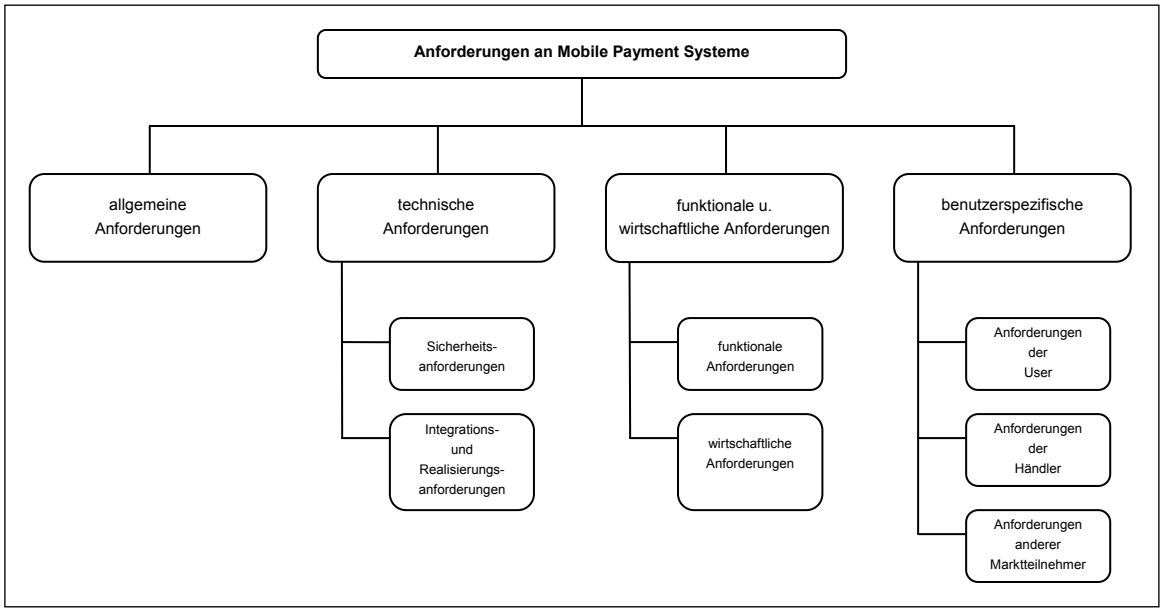

Abbildung 9: Anforderungen an Mobile Payment Systeme

- **Independence (Unabhängigkeit)** drückt aus, dass sich verschiedene mobile Zahlungstransaktionen untereinander nicht beeinflussen.

- **Durability (Dauerhaftigkeit)** stellt dar, dass Daten und Informationen mobiler Zahlungstransaktionen bei Verlust, Defekt oder Diebstahl im System wieder hergestellt werden können bzw. müssen.

- **Reputation und Reliability (Verlässlichkeit)** drücken aus, dass Mobile Payment Systeme vertrauenswürdig sind und auf Dauer existieren müssen.

- **Ubiquity (Allgegenwärtigkeit/Erreichbarkeit)** bezeichnet, dass Mobil Payment Systeme allgegenwärtig in jeder Situation und ständig erreichbar sein müssen.[242]

- **Availability (permanente Verfügbarkeit)** bedeutet, dass Mobile Payment Systeme zeitlich ununterbrochen zur Nutzung verfügbar sein müssen.

[242] Vgl. Pößneck (2006); Zhou/Bergmann/Schlang (2004), S. 24.

- **Privacy (Datenschutz und Privatsphäre)** besagt, dass Mobile Payment Systeme Datenschutz und Privatsphäre der Personen gewährleisten müssen. User können in der Lage sein, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen (Informationelle Selbstbestimmung des Users), wobei die User-Anonymität als eine optionale Möglichkeit für den Schutz der Privatsphäre gegeben sein muss.[243]

- **Internationality (Internationalität)** bedeutet, dass eine grenzüberschreitende Möglichkeit mobiler Zahlungen besteht. Die Internationalisierung und Globalisierung von Märkten erfordern die grenzüberschreitende Nutzung der Mobile Payment Systemen. Deshalb müssen Mobile Payment Systeme auch dieser Anforderung gerecht werden.

- **Development (Entwicklung)** bezeichnet, dass Mobile Payment Systeme ein hohes Entwicklungspotential in sich tragen sollen. Auf diese Weise können die Zahlungssysteme große Akzeptanz bei den Usern und Händlern finden und mehr Vertrauen gewinnen.

Die allgemeinen Anforderungen an Mobile Payment Systeme werden in den folgenden Abschnitten ausführlich erklärt.

3.2.2 Technische Anforderungen

An Mobile Payment Systeme werden einige technische Anforderungen gestellt, um technisch störungsfreie mobile Zahlungstransaktionen zwischen den Marktteilnehmern zu gewährleisten. Ein Mobile Payment System soll eine technische Sicherheit anbieten, wenn es bei einer mobilen Zahlungstransaktion zu einer Störung oder gar einer Unterbrechung oder einem Abbruch kommt. Zudem soll ein Mobile Payment System einen Schutz gegen An- und Zugriffe wie Überwachung oder Manipulation von Daten durch Dritte anbieten. Schließlich soll ein Mobile Payment System eine einfache Installation und Konfiguration beinhalten, da sich die User dadurch die Sicherheitslücken wie Trojaner, Spyware, Virus etc. in Browsern, Anwendungen und Betriebssystemen befürchten.[244] Im Folgenden werden die hier kurz

[243] Vgl. Garstka (2003), S. 48, 52ff.

[244] Vgl. Karnouskos/Hoepner/Holzmann-Kaiser (2003), S. 3.

erläuterten Anforderungen detailliert dargestellt. Zunächst werden die Sicherheitsanforderungen, dann die Integrations- und Realisierungsanforderungen erläutert.[245]

3.2.2.1 Sicherheitsanforderungen

Die Sicherheitsanforderungen betreffen die technische Sicherheit der Mobile Payment Systeme gegen Störungen und den Schutz dieser Systeme und Marktteilnehmer gegen unberechtigte Zugriffe, Manipulation, Überwachung und Abhören. Die Sicherheitsanforderungen können wie folgt erläutert werden:[246]

Availability (Verfügbarkeit) und Reliability (Zuverlässigkeit): Ein Mobile Payment System soll jederzeit verfügbar sein, wenn die User eine Zahlungstransaktion ausführen oder eine Zahlung empfangen möchten. Dies ist gewährleistet, wenn die Funktionalität von Mobile Payment Systemen z. B. nicht durch Hard- und Softwarefehler oder durch Katastrophen oder Sabotage etc. beeinträchtigt werden kann.[247] Dabei soll das Mobile Payment System zuverlässig sein, um eine Zahlungstransaktion vollständig abwickeln zu können.[248]

Confidentiality (Vertraulichkeit): Die User- bzw. Transaktionsdaten und -informationen dürfen nur den beteiligten Parteien bekannt sein und müssen gegenüber Dritten vertraulich behandelt werden. Diese Daten und Informationen können nicht durch unautorisierte Personen, Instanzen oder Prozesse eingesehen werden. Bei der Vertraulichkeit ist neben dem Datenschutz auch von der User-Anonymität die Rede, die in den nächsten Abschnitten näher erklärt wird.[249] Insbesondere personenbezogene Userdaten und -informationen wie z. B. Name, Mobilfunknummer, Adresse etc. müssen anonym bleiben, da durch diese Daten und Informationen Userprofile erstellt werden.[250]

---

[245] Vgl. Illik (2002), S. 179ff.

[246] Vgl. o. V. (2010b); Adamec et al. (2009), S. 23; Karnouskos/Hoepner/Holzmann-Kaiser (2003), S. 3. Vgl. Himmelspach et al. (1996), S. 2; Illik (2002), 179ff.

[247] Vgl. o. V. (2010b).

[248] Vgl. Illik (2002), S. 179.

[249] Vgl. o. V. (2010b) und mit den Erläuterungen im Abschnitt 3.2.2.2 Integrations- und Realisierungsanforderungen, S. 68 sowie im Abschnitt 3.2.4.1 Anforderungen der mobilen User, S. 72.

[250] Vgl. Himmelspach et al. (1996), S. 2; Illik (2002), S. 180; Die Differenzierungen zwischen Daten und Informationen werden im Abschnitt 5.1 Organisatorische Rahmenbedingungen der User-

Fortsetzung auf der nächsten Seite

Integrity (Integrität): Dies umfasst die Integrität der Daten und Systeme.[251] Die Transaktionsdaten und -informationen müssen zwischen den beteiligten Parteien unversehrt übertragen werden. Das heißt, die Informationen müssen für alle identisch sein, so dass eine Änderung oder Zerstörung durch Dritte ausgeschlossen ist. Beispielsweise werden digitale Signaturen zur Gewährleistung der Integrität von Daten und Informationen eingesetzt.[252] Neben der Datenintegrität muss auch die Systemintegrität gewährleistet sein, so dass ein Mobile Payment System nicht durch unautorisierten Zugang manipuliert werden kann.[253]

Authenticity (Authentizität/Verifikation): Dies beschreibt die Verifikation der Identität eines Subjektes, wobei ein Subjekt ein User, ein Prozess, ein System oder eine Information sein.[254] Die Identität von beteiligten Transaktionspartnern muss durch ein Verifizierungsverfahren geprüft werden. Zusätzlich werden digitale Signaturen und Zertifikate für die Authentisierung bzw. die Erhöhung der Sicherheit benutzt. Bei der Authentisierung ist die Anonymität von Usern nicht gegeben, aber z. B. durch die Anonymisierung oder Pseudonymisierung kann ein bestimmter Grad an Anonymität erreicht werden.[255]

Authorization (Autorisierung/Zugriffskontrolle): Bei der Autorisierung wird die Zugriffsberechtigung auf die User- und Transaktionsdaten bestimmt und somit ein unberechtigter Zugriff auf diese Daten verhindert.[256]

Non-Repudiation (Nicht-Abstreitbarkeit/Verbindlichkeit): Die Non-Repudation, auch als Verbindlichkeit einer Kommunikation bezeichnet, bedeutet, dass eine Nachricht zwischen den Transaktionspartnern (Sender und Empfänger) gesendet und empfangen wurde. Die Nicht-Abstreitbarkeit ist somit eine Möglichkeit, um zu beweisen, dass zu einem bestimmten Zeitpunkt eine Kommunikation zwischen zwei Partnern stattgefunden hat.[257] Danach können weder Sender noch Empfänger später

---

Anonymität, S. 113ff. erklärt sowie weitere Erläuterungen über die personenbezogenen Daten und Informationen erfolgen im Abschnitt 5.1.1 User- und Geschäftsdaten und Informationen, S. 114ff.

251 Vgl. o. V. (2010b).

252 Die Transaktionsdaten und -informationen werden im Abschnitt 5.1.4 Verbindungsdaten und Transaktionsdaten, S. 119ff. ausführlich erläutert.

253 Vgl. o. V. (2010b); Himmelspach et al. (1996), S. 2 und 3; Illik (2002), S. 180;

254 Vgl. Ebenda.

255 Vgl. BSI (2006), S. 46 sowie mit den Erläuterungen im Kapitel 4 Grundlagen der Anonymität, S. 81ff. In diesem Kapitel wird diese Anforderung ausführlich erläutert.

256 Vgl. Himmelspach et al. (1996), S. 3; Illik (2002), S. 180;

257 Vgl. Wohlmacher (2000), S. 1, 2 und 8ff.; Keller/Meier/Schumacher (2002), S. 3.

erfolgreich abstreiten, dass die Nachricht nicht gesendet bzw. empfangen wurde.[258] Das wird in einer Kommunikationsbeziehung für die Verifizierung der Vertrauenswürdigkeit von digitalen Signaturen eingesetzt.[259] Die Nicht-Abstreitbarkeit beinhaltet auch die Eigenschaften der Authentizität und der Integrität.[260]

Schutz gegen die Angriffe: Ein Mobile Payment System muss in der Lage sein, sich gegen die potentiellen Angriffe wie z. B. Manipulation, Spionage, Sabotage oder Phishing etc.[261] auf den Transaktionsprozess und -daten abzuwehren.

3.2.2.2 Integrations- und Realisierungsanforderungen

Die Integrations- und Realisierungsanforderungen beschreiben die Gestaltungsprinzipien der Mobile Payment Systeme in mobiler Umgebung der Marktteilnehmer.[262]

Technische Integrationsfähigkeit: Ein Mobile Payment System soll aus technischer Sicht integrationsfähig sein, um sich leicht in userspezifische sowie betriebliche IT-Infrastrukturen und Applikationen einfügen zu lassen.[263]

Technische Einfachheit und Sicherheit: Technische Realisierung der Systemintegration in userspezifische und betriebliche IT-Infrastrukturen soll einfach und sicher gewährleistet werden. Die Kommunikation zwischen den beteiligten Transaktionspartnern wird durch die standardisierten Schnittstellen und Transaktions-

---

258 Vgl. Swoboda/Spitz/Pramateftakis (2008), S. 17.

259 Vgl. Wohlmacher (2000), S. 8ff.; Illik (2002), S. 181.

260 Vgl. Swoboda/Spitz/Pramateftakis (2008), S. 17; Himmelspach et al. (1996), S. 4.

261 Durch Manipulation von Hard- oder Software verschafft sich ein Fremder Vermögensteile, beispielsweise durch Veränderung von Gehalts- oder Kontodaten. Bei Spionage verschafft sich ein Täter Zugang zu besonders gesicherten Datenbeständen oder Programmen, beispielsweise durch Kopieren von Personen-, Kunden- oder Forschungs- und Entwicklungsdaten. Sabotage bezeichnet die Zerstörung von Datenbeständen sowie die Beeinträchtigung von Verarbeitungsabläufen. Das sind strafbare Handlungen und werden in Deutschland mit Geldstrafe und Freiheitsstrafen bis zu fünf Jahren bestraft. Vgl. mit dem Abschnitt „Computerkriminalität“ in: Abts/Mülder (2009), S. 428. Bei Phishing (Kurzform vom „Passwort fischen“) versuchen Betrüger, über gefälschte Emails oder Internet-Adressen an die persönlichen Daten eines Users z. B. Passwörter oder Transaktionsnummer (TAN) zu kommen. Vgl. Ebenda, S. 438.

262 Vgl. Karnouskos/Hoepner/Holzmann-Kaiser (2003), S. 3.

263 Vgl. Himmelspach et al. (1996), S. 5; Illik (2002), S. 182.

datenformate einfacher und durch die kryptografischen Verschlüsselungsmethoden sicherer.[264]

Systemoffenheit und Plattformunabhängigkeit: Ein Mobile Payment System muss sich als ein offenes System darstellen, so dass dies unabhängig von einer bestimmten Software und Hardware ist, um die Marktteilnehmer nicht zu beschränken und neuen Marktteilnehmern Zugang zum System zu schaffen. Dabei soll ein Mobile Payment System in der Lage sein, plattformunabhängig bei den beteiligten Transaktionssystemen zu funktionieren.[265]

Datenschutz-Safety: Die Zahlungsdaten und -informationen von Usern und Händlern müssen sicher gespeichert sein, um diese gegen möglichen unbeabsichtigten Unfälle und Verluste z. B. Zerstörung oder Schädigung der Einrichtungen, fahrlässiges oder nachlässiges Verhalten der Mitarbeiter etc. schützen zu können.[266]

Datenschutz-Security: Die personenbezogenen Daten wie Username, -adresse und Kreditkartennummer etc. und Transaktionsdaten müssen verschlüsselt auf einem separaten Server, der vom Internet durch eine Firewall o. ä. getrennt ist, gespeichert werden, um mögliche und potentielle Schädigungen des Systems z. B. durch Missbrauch, Diebstahl etc. auszuschließen. Hier müssen diese personenbezogenen Daten und Transaktionsdaten durch den Einsatz von kryptographischen Verfahren verschlüsselt werden, um bei den Teilnehmern Vertrauen zu schaffen. Auf der anderen Seite besteht die Gefahr, dass diese personenbezogenen Daten und Transaktionsdaten mehrfach bei verschiedenen Händlern oder Payment Service Providern existieren und dass dadurch Rückschlüsse auf Userprofile und deren Konsumverhalten gezogen werden können.[267]

---

[264] Vgl. Himmelspach et al. (1996), S. 5; Illik (2002), S. 184.

[265] Vgl. Himmelspach et al. (1996), S. 9.

[266] Zur Unterscheidung von Safety von Security: Safety bezieht sich auf die Zuverlässigkeit eines Systems, speziell in Bezug auf dessen Ablauf- und Ausfallsicherheit (Umgebungssicherheit). Security bezeichnet dagegen den Schutz eines Systems vor beabsichtigten Angriffen (Sicherheit gegegen absichtliche Angriffe). Die beiden Begriffe sind nicht völlig unabhängig voneinander: Safety schließt auch Security mit ein, was bedeutet, dass ohne einem gewissen Level an Security keine ausreichenden Safety Eigenschaften erzielt werden können. Vgl. Sternberger (2003), S. 3; Vgl. Himmelspach et al. (1996), S. 9 und 10.

[267] Vgl. Himmelspach et al. (1996), S. 10.

Vermeidung von Geldverlust: Ein Mobile Payment System muss so konstruiert sein, dass ein Geldverlust durch System- oder Userfehler vermieden wird. Das heißt, ein Mobile Payment System muss entsprechende Recovery- und Sicherheitsfunktionen haben, wenn bei einer Zahlungstransaktion ein technischer Defekt, versehentliche Löschung oder Missbrauch von Zahlungsmittel entsteht.

Zusätzliche Hardware und Software: Ein Mobile Payment System soll möglichst ohne zusätzliche bzw. mit weniger Hardware wie Kartenleser oder Terminal für Smartcards und Software wie z. B. Online-Banking und Payment-Anwendungen auskommen.[268]

3.2.3 Funktionale und wirtschaftliche Anforderungen

3.2.3.1 Funktionale Anforderungen

Die funktionalen Anforderungen betreffen die Nutzungsmöglichkeiten der Mobile Payment Systeme in mobiler Umgebung der Marktteilnehmer.[269]

Konvertibilität: Konvertibilität bezeichnet die Möglichkeit, die eigene Währung frei und ungehindert in fremde Währung zum allgemein gültigen Wechselkurs umzutauschen.[270] Ein Mobile Payment System kann durch eine Funktionalität wie Konvertibilität für die Marktteilnehmer flexibler gestaltet werden. So können die Händler ihre Kundenbasis erweitern. Die User können dann ihr elektronisches Geld zwischen den Zahlungssystemen leichter konvertieren.

Übertragbarkeit: Ein Mobile Payment System muss die Übertragung von Geldern nicht nur zwischen den Usern und Händlern (B2C), sondern auch zwischen den Usern (P2P) untereinander unterstützen. Beispiel: PayPal Mobile.[271]

---

[268] Vgl. Himmelspach et al. (1996), S. 2; Zhou/Bergmann/Schlang (2004), S. 23.

[269] Vgl. Karnouskos/Hoepner/Holzmann-Kaiser (2003), S. 3; Himmelspach et al. (1996), S. 11.

[270] Konvertibilität bezeichnet die Möglichkeit, die eigene Währung frei und ungehindert in fremde Währung zum allgemein gültigen Wechselkurs umzutauschen. Auch die unbeschränkte Transferierbarkeit inländischer Währung ins Ausland bzw. ausländischer Währung ins Inland zählt zu den Konvertibilitätsmerkmalen. Als voll konvertibel gelten nur Währungen, die weder für Inländer noch für Ausländer Beschränkungen des laufenden zwischenstaatlichen Zahlungs- und Kapitalverkehrs aufweisen. Der Euro ist eine solche voll konvertible Währung. Vgl. http://www.bundesbank.de/bild-ung/bildung_glossar_k.php, Stand: 28.02.2010.

[271] Vgl. https://www.paypal.com/mobile, Stand: 29.01.2010.

Quittung/Rückerstattung: Ein Mobile Payment System muss bei Transaktionen eine Quittungsfunktion für eventuellen Umtausch, Versteuerung und Garantie bieten. Wenn der User mit der Ware unzufrieden ist, muss er dann in der Lage sein, eine Rückerstattung zu fordern.[272]

Eignung für Micro Payments: Ein Mobile Payment System muss auch die Möglichkeit bieten, Einkäufe mit kleineren Beträgen (Micro Payments) tätigen zu können, da viele Produkte im Netz sehr wenig kosten, z. B. Download einzelner Songs.[273]

3.2.3.2 Wirtschaftliche Anforderungen

Die wirtschaftlichen Anforderungen beschreiben die Kosten der Nutzung der Mobile Payment Systeme in mobiler Umgebung der Marktteilnehmer.[274]

Zahlungssystem- und Transaktionskosten: Mobile Payment Systeme verursachen Transaktionskosten für die Händler und User in Form der Konto- oder Transaktionsgebühren. Deshalb soll ein Mobile Payment System bei einer Transaktion so günstig sein, dass die Kosten im akzeptablen Rahmen bleiben. So fallen für die User meistens einmalige Registrierungsgebühren und zeit- oder nutzungsabhängige Gebühren an. Für den Händler entstehen auch Kosten für Setup und Kontoführung beim Payment Service Provider. Darüber hinaus entstehen Installations- und Wartungskosten sowie Aufwendungen für Hard- und Software, Mahn- und Inkassokosten und Kommunikationskosten. Der Datentransfer in Mobile Payment Systemen soll ebenfalls möglichst schnell verarbeitet werden, um Transaktionskosten bei den beteiligten Transaktionspartnern zu vermeiden.[275]

Eignung für bestimmte Einkäufe: Ein Mobile Payment System soll über solche Gebührenmodelle verfügen, die das Mobile Payment System attraktiv für die User und Händler machen. Bei Micro Payments sind die Zahlungsbeträge in kleinem Cent-Bereich, so dass die Gebühren den Zahlungsbetrag überschreiten können. Deshalb sollen die Gebühren niedriger sein als der Wert der Ware. Ein Lösungsvorschlag für die Gestaltung der Gebühren wäre die Festlegung eines Mindestumsatzes oder einer

---

[272] Vgl. Himmelspach et al. (1996), S. 11 und 12; Illik (2002), S. 185.
[273] Vgl. Himmelspach et al. (1996), S. 12; Illik (2002), S. 187.
[274] Vgl. Karnouskos/Hoepner/Holzmann-Kaiser (2003), S. 3.
[275] Vgl. Himmelspach et al. (1996), S. 12ff.

Mindestmenge, wobei die Gebühren die Attraktivität des Einkaufes nicht beeinträchtigen sollte.[276]

3.2.4 Benutzerspezifische Anforderungen

Die benutzerspezifischen Anforderungen betreffen die einzelnen Anforderungen der User, Händler und anderen Marktteilnehmern wie Mobilfunknetzbetreiber, Banken und der Staat.[277]

3.2.4.1 Anforderungen der mobilen User

Eine Übersicht für die einzelnen Anforderungen der User geben Himmelspach et al. (1996) sowie Henkel (2001) in ihren Untersuchungen für die elektronischen Zahlungssysteme.[278] Im Zusammenhang mit der Mobilität der User, dem Mobile Commerce bzw. Mobile Payment existieren weitere Untersuchungen, in denen die Anforderungen der mobilen User analysiert wurden.[279] In der Abbildung 10, S. 74 werden Kriterien für die Akzeptanz von Mobile Payments dargestellt, die im Rahmen einer empirischen Untersuchung der Kundensicht auf Mobile Payment-Verfahren ermittelt wurden.[280] Die befragten Personen haben angegeben, dass sie einen vertraulichen Umgang mit persönlichen Daten (96,2 %) erwarten und der Bezahlvorgang anonym (65,6 %) ablaufen und keine Anmeldung nötig (45,5 %) sein soll. Danach soll ein Mobile Payment System folgende Anforderungen der mobilen User erfüllen:[281]

---

[276] Vgl. Ebenda, S. 16.

[277] Vgl. Himmelspach et al. (1996), S. 17; Illik (2002), S. 187.

[278] Vgl. Himmelspach et al. (1996), S. 17; Henkel (2001), S. 4.

[279] Vgl. Khodawandi/Pousttchi/Wiedemann (2003); Zhou/Bergmann/Schlang (2004).

[280] Ende 2002 wurde von den Wissenschaftlern an der Universität Augsburg eine empirische Untersuchung der Kundensicht auf Mobile Payment-Verfahren mit drei Hauptzielen durchgeführt: 1. die Gründe für die Nutzung oder Ablehnung offen zu legen, 2. die Relevanz der unterschiedlichen Bezahlszenarien zu ermitteln, 3. das Gewicht der einzelnen Akzeptanzkriterien zu bestimmen. Vgl. Khodawandi/Pousttchi/Wiedemann (2003).

[281] Vgl. Ebenda; Himmelspach et al. (1996), S. 17ff.

Datenschutz: Im Zusammenhang mit dem vertraulichen Umgang mit persönlichen Daten erwarten User einen Schutz vor Missbrauch, Manipulation, Verlust und Diebstahl von Transaktionsdaten und userspezifischen Informationen.[282]

Anonymität: Ein Mobile Payment System soll einen bestimmten Grad an User-Anonymität gewährleisten. Die Händler können mit Hilfe der gespeicherten Informationen Kundenprofile erstellen und gegenüber den Usern eine bessere Position und Marktmacht erhalten. Wie im Abschnitt 2.7 Anwendungsbereiche von Mobile Payments, S. 41 bereits erläutert, bezahlt der mobile User in verschiedenen Situationen. Der User kann jedoch in bestimmten Situationen anonym bleiben bzw. anonym bezahlen wollen. Beispielsweise können vom User, wenn er in verschiedenen Städten reist und dort parkt, anhand der hinterlassenen Daten Bewegungsprofile erstellt werden, wo er sich aufgehalten, geparkt und bezahlt hat. Der mobile User ist nicht mehr anonym. Deshalb erwarten mobile User, wie im Bargeldverkehr, anonyme Zahlungen tätigen zu können.[283] Die Fragen diesbezüglich sind: Was braucht der mobile User, damit er mobil und anonym bezahlen kann? Muss er alle personenbezogenen Daten an die anderen Marktteilnehmer senden? Wie kann er in bestimmten Situationen anonym bezahlen? Was sind seine Interessen im datenschutzrelevanten Sinne? Diese Fragen werden in diesem Abschnitt sowie in den nächsten Kapiteln beantwortet.[284]

Mobile Payment Systeme können derzeit entweder keine oder nur partielle User-Anonymität gewährleisten, wie z. B. bei Kreditkarten. Daher sollten Mobile Payments einen bestimmten Grad der Anonymität mobiler User gewährleisten können.[285]

Verfügbarkeit/Verlässlichkeit: Ein Mobile Payment System soll gewährleisten, dass die Abwicklung des Zahlungsvorgangs problemlos und jederzeit durchgeführt werden kann. Die Programme sollten regelmäßig gewartet werden und sicher laufen.[286]

---

[282] Vgl. mit den Datenschutzanforderungen im Abschnitt 3.2.2.2 Integrations- und Realisierungsanforderungen, S. 68.

[283] Vgl. Jain/Seri/Srinivasan (2008), S. 21.

[284] Vgl. mit den Erläuterungen im Kapitel 4 Grundlagen der Anonymität, S. 81 und im Kapitel 5 Rahmenbedingungen der User-Anonymität, S. 113 sowie im Kapitel 6 User-Anonymität in Mobile Payment Systemen, S. 153.

[285] Vgl. Illik (2002), S. 187. Auf diese Thematik wird im Kapitel 4 Grundlagen der Anonymität, S. 81 und 6 User-Anonymität in Mobile Payment Systemen, S. 153 näher eingegangen.

[286] Vgl. Zhou/Bergmann/Schlang (2004), S. 23.

Vertrauen: Eine wesentliche Anforderung an Mobile Payment Systemen ist die Sicherung des Vertrauens der einzelnen User.[287] Dieses Vertrauen kann beispielsweise durch die Zertifizierung von Händlern bzw. Webshops durch einen Dritten erhöht werden.[288] Dabei sollen sowohl Händler als auch Payment Service Provider Vertrauen bei den Usern schaffen.

Schutz vor Diebstahl, Verlust und Betrug: Mobile Payment Systeme sollen einen Schutz vor Verlust und Diebstahl des Zahlungsmittels sowie einen Schutz vor Betrug durch Händler oder Payment Service Provider gewährleisten.

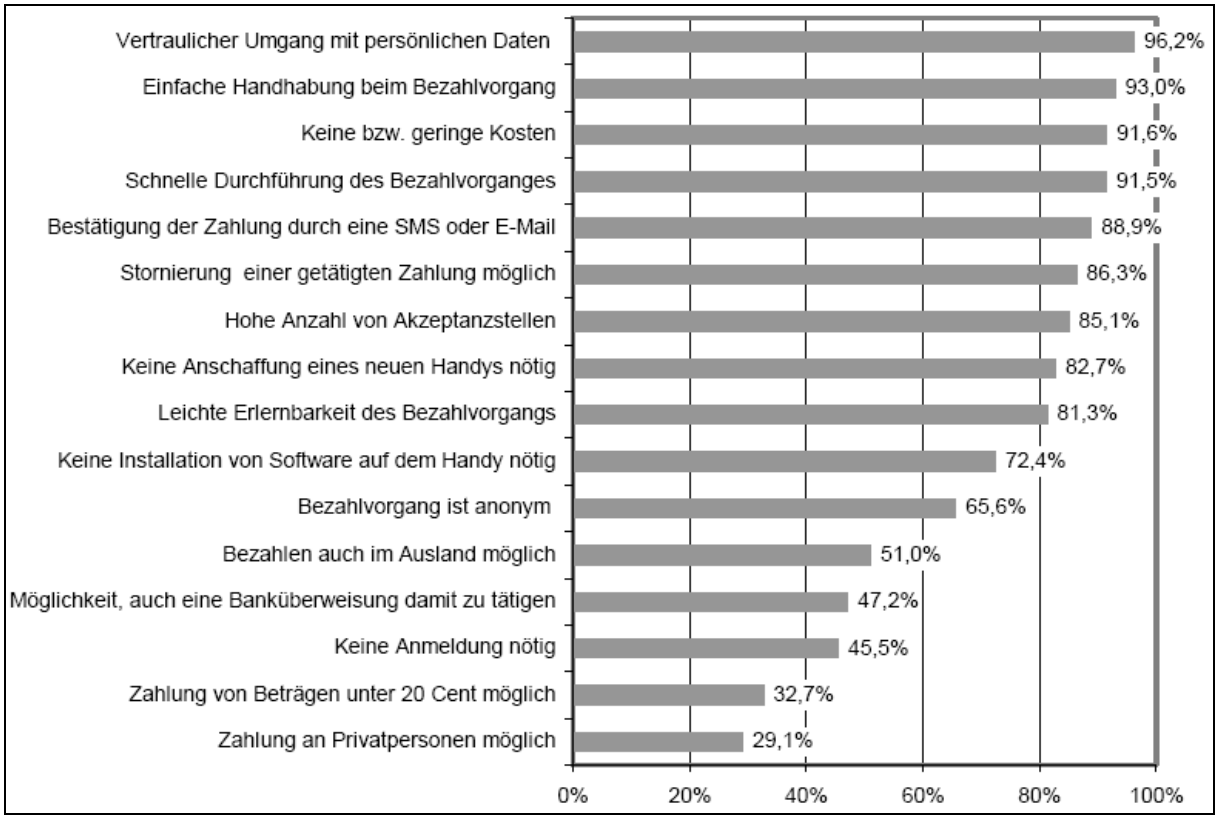

Abbildung 10: Kriterien für die Akzeptanz von Mobile Payments[289]

Userfreundlichkeit: Unter Userfreundlichkeit (Convenience) wird die komfortable und einfache Bedienung des Systems durch die User verstanden. Ein Mobile Payment System soll den Usern neben den Zahlungsmöglichkeiten auch zusätzliche Dienste wie z. B. individuelle oder allgemeine Beratung, Online-Hilfe-Stellung, Downloadbereiche für Aktualisierung von Payment System etc. bieten. Die Mobile

[287] Vgl. Ebenda.

[288] Vgl. mit dem Abschnitt 3.1.7 Trusted Third Party, S. 60.

[289] Vgl. Khodawandi/Pousttchi/Wiedemann (2003), S. 42.

Payment Services sollen weitverbreitet bei den Händlern verfügbar und einfach bedienbar sein. Mobile User fordern an, dass ihre Involvierung im Mobile Payment Prozess gering ist. Damit sie immer in der Lage sind, den aktuellen Status ihrer Zahlungstransaktionen abzurufen, möchten sie eine Übersicht ihrer Zahlungstransaktionen in Echtzeit haben.[290]

Ubiquität/Flexibilität: Mobile User möchten in der Lage sein, Mobile Payments zeit-, ort- und währungsunabhängig zu tätigen. Der mobile User möchte neben den B2C-Einkäufen auch P2P-Zahlungstransaktionen wie z. B. Überweisungen, durchführen.[291]

Kosten: Die Nutzung von Mobile Payment Services soll möglichst geringe bis keine Kosten verursachen. Die Konditionen für die Nutzung von Mobile Payment Systemen sollen günstiger als die der herkömmlichen Zahlungssysteme gestaltet werden. Im Vergleich zu herkömmlichen Zahlungssystemen soll der User weniger Zeit für die Durchführung mobiler Zahlungstransaktionen brauchen.[292]

Hard- und Software: Mobile Payment Systeme sollen möglichst ohne eine Installation von Hard- oder Software bei den Usern auskommen. Der User soll nicht viel zusätzlich in die Hard- oder Software wie z. B. Barcodeleser-Software investieren müssen, um Mobile Payments zu nutzen.[293]

3.2.4.2 Anforderungen der Händler

Auf der anderen Seite gibt es die Interessen und Anforderungen der Händler und MCP an Mobile Payment Systeme. Dabei stellen die Händler die folgenden Anforderungen an Mobile Payment Systemen:[294]

Investitions- und Transaktionskosten: Mobile Payment Systeme sollten geringen technischen Aufwand erfordern und keine oder geringe Investitionskosten verursachen. Außerdem fordern Händler niedrige Transaktionskosten. Daher sollen

---

290 Vgl. Himmelspach et al. (1996), S. 17 und 18; Illik (2002), S. 188; Zhou/Bergmann/Schlang (2004), S. 23.

291 Vgl. Zhou/Bergmann/Schlang (2004), S. 24.

292 Vgl. Ebenda, S. 23.

293 Vgl. Ebenda.

294 Vgl. Himmelspach et al. (1996), S. 19 und 18; Illik (2002), S. 188; Zhou/Bergmann/Schlang (2004), S. 23.

Mobile Payment Systeme mit kurzen und damit akzeptablen Transaktionszeiten funktionieren. Die Kosten für Mobile Payment Transaktionen sollen auf einem akzeptablen Niveau sein.[295]

Auswertbarkeit: Händler möchten wissen, wer bei ihnen Produkte oder Services kauft. Hier möchte er gerne möglichst viele Informationen über die Einkäufe und Kunden sammeln und diese nutzen. Normalerweise bekommen Händler und Content Provider eine große Menge Daten und Informationen, die sie im Rahmen der Datenschutzregelungen beliebig analysieren können.[296]

Interoperabilität: Die Händler erwarten, dass das Mobile Payment System interoperative kompatible Transaktionsgeräte und –systeme hat und mit anderen Systemen reibungslos funktioniert.

Vertrauen/Kundenloyalität: Mobile Payment Services sollen hohe Sicherheit und Vertrauen bieten. Diese Systeme sollten auch ermöglichen, die Mobile Payment Services anzupassen, wenn neue Services beispielsweise Treue- oder Bonusprogramme zu den vorhandenen Services kommen. Der Status mobiler Zahlungstransaktionen sollte in Echtzeit abrufbar sein.

Integration in den Geschäftsprozess: Die Integration des Mobile Payment Systems in den Geschäftsprozess bzw. in die neuen oder existierenden Systeme soll ebenso wie die Installation von Hard- und Software einfach sein. Dabei möchte der Händler einen reibungslosen Austausch von Transaktionsinformationen zwischen eigenen und anderen Servern.[297]

Risikomanagement: Mobile Payment Systeme sollen ein Risikomanagement-Instrument für die Minimierung von technischen, wirtschaftlichen und rechtlichen Risiken besitzen. Das Serversystem muss gegen Angriffe oder Manipulation durch Dritte ausgerüstet und protektiert werden. Beispielsweise kann ein solches Risikomanagement durch entsprechende Sicherheitsmaßnahmen wie z. B. durch die Installation und Wartung von Firewalls, Anti-Spy und Virusscan gegen die Attacken von außen und durch Vergabe von User- und Zugriffsrechte und interne Sicherheitsmaßnahmen wie z. B. Zutrittsrechte für die Serverräumlichkeiten organisiert

---

[295] Vgl. Himmelspach et al. (1996), S. 12 und 20.

[296] Datenschutzregelungen sowie weitere rechtliche Bestimmungen werden im Abschnitt 5.3 Regulatorische Rahmenbedingungen der Anonymität, S. 140 näher erläutert.

[297] Vgl. Himmelspach et al. (1996), S. 19; Illik (2002), S. 188.

werden.[298] Ebenfalls fordern Händler ein effektives Instrument für die wirtschaftlichen Risiken wie z. B. Betrugs- und Zahlungsausfälle. Zudem können durch die fehlenden Standards oder Technologieänderungen finanzielle Risiken entstehen, wie z. B. hohe Investitionskosten.[299] Rechtliche Risiken können z. B. durch fehlende Rechtsvorschriften oder in den Haftungsfragen bei einer Nichterfüllung bzw. mangelhafter Erfüllung der Leistung entstehen.[300]

Verbreitung und Marktdurchdringung: Mobile Payment Systeme können Händlern helfen, in tiefere Marktsegmente einzudringen und damit ihre Marktposition zu stärken. Beispielsweise können Händler vorhandenen Kunden Mobile Payments als weitere Zahlungsmöglichkeiten anbieten und diese besser bedienen sowie gleichzeitig neue Zielgruppen im Mobile Commerce, die z. B. Location-based Services nutzen, gewinnen.[301]

3.2.4.3 Anforderungen anderer Marktteilnehmer

In diesem Abschnitt werden die Anforderungen sowie Interessen der Mobilfunknetzbetreiber, der Banken und Kreditinstitute sowie des Staates bzw. der Regulierungsbehörden an Mobile Payment Systeme erläutert.

Mobilfunknetzbetreiber betrachten Mobile Payments als strategischen Mehrwert-Service neben ihren anderen existierenden Services, der die Kundenbindung und –treue ermöglicht. Dadurch schaffen Mobile Payment Systeme zusätzliche Einnahmequellen für die Mobilfunknetzbetreiber und steigern den Durchschnittsertrag pro Kunde.[302] Mobilfunknetzbetreiber können ihre bestehenden Billing-Systeme zur Abrechnung von Einkäufen und Erwerb von Dienstleistungen nutzen. Dabei haben sie einen direkten Zugang zu den Daten einer breiten Userbasis. Diese Userbasis können sie für die verschiedenen Marketingmaßnahmen nutzen und die User gezielt ansprechen. Mobilfunknetzbetreiber haben großes Interesse an Mobile Payment auf der Basis von Mobiltelefonen, da sie vom Mobilfunknetzbetreiber zum Mobile Service Integrator entwickeln und neue innovative Services für die User u.a. Mobile Payment

---

[298] Vgl. Ebenda.

[299] Vgl. mit der Rubrik „Investitions- und Transaktionskosten“, S. 75.

[300] Vgl. Himmelspach et al. (1996), S. 19 und 20; Illik (2002), S. 188.

[301] Vgl. mit den Erläuterungen im Abschitt 2.1.2 Location Based Services, S. 14.

[302] Vgl. Zhou/Bergmann/Schlang (2004), S. 30.

Services anbieten werden. Sie erwarten deshalb z. B. einen großen Erfolg der Near Field Communication basierend auf der RFID-Technologie.[303]

Banken und Kreditinstitute möchten Kunden sichere und vertrauenswürdige Mobile Payment Services anbieten und erwarten dabei die Verluste, die durch Betrug entstehen, zu minimieren. Die technische Integration von Mobile Payment Services sollte in die neuen und existierenden Infrastrukturen möglich sein. Beispielsweise können ihre eigenen Payment Systeme im Alleingang oder in einer Kooperation mit den anderen Teilnehmern auf den Markt bringen. Auf dieser Weise können Banken und Kreditinstitute ihr Finanzproduktspektrum erweitern und die bestehenden Infrastrukturen besser auslasten. Insbesondere Kreditkartengesellschaften und Banken möchten ihre Position im mobilen Zahlungsverkehr sichern bzw. erweitern. Sie möchten Ihre Instituts- und Produktmarken neu orientieren und die Kundenloyalität erhöhen.

Staat bzw. Regulierungsbehörden stellen folgende Anforderungen an Mobile Payment Systeme: [304]

Nicht-Duplizierbarkeit des Geldes: Ein Mobile Payment System soll eine sicherheitstechnische Komponente gegen die Nicht-Duplizierbarkeit des elektronischen Geldes haben. Beispielsweise können diese durch die Verschlüsselung von elektronischen Münzen oder des elektronischen Geldversprechens sowie Authentisierung von Marktteilnehmern und Münzen gesichert werden.[305]

Gelderstellung und Kontrolle durch die Zentralbank oder Regierung: Der Staat kann durch seine Zentralbank oder ähnlichen Instanzen die Gelderstellung und -ausgaben für eine sichere Umgebung sorgen, so dass keine kriminelle Aktivitäten wie Geldwäsche oder Betrug vorkommen.[306]

Zusammenfassend kann festgehalten werden, dass die Marktteilnehmer unterschiedliche Interessen und Anforderungen haben, die aus der Perspektive der einzelnen Marktteilnehmer berechtigt sind. Zu erwähnen gilt es jedoch, dass auch einige Konflikte zwischen den einzelnen Anforderungen bestehen. Konflikte bestehen be-

---

303 Vgl. Ondrus/Pigneur (2006), S. 3 und mit dem Abschnitt 2.6.2.1 Near Field Communication, S. 36.

304 Vgl. Himmelspach et al. (1996), S. 20; Illik (2002), S. 189 und mit dem Abschnitt 3.1.8 Staat, S. 62.

305 Vgl. Ebenda.

306 Vgl. Ebenda.

sonders zwischen Sicherheit und Einfachheit sowie zwischen eindeutiger Identifikation und Anonymität. Während die Mobile Payment Systeme eine Sicherheit für die Gefahren und Risiken bieten sollen, sollen diese Systeme in der Handhabung einfach und anonym für die User gestaltet werden, wobei die Anforderungen der Händler und anderer Marktteilnehmer ebenfalls berücksichtigt werden sollen. Sonst besteht die Gefahr, dass das Mobile Payment System nicht von den Usern und Händlern akzeptiert wird. Eine einseitige Ausrichtung an einen Marktteilnehmer würde die Akzeptanz und Gestaltung von Mobile Payment Systemen in die Irre führen. Bisherige Erfahrungen mit den Mobile Payment Systemen zeigen jedoch, dass ein Mobile Payment System nur dann Erfolg haben kann, wenn es für alle Marktteilnehmer einen relativen Zusatznutzen bietet sowie eine Alternative zu den herkömmlichen Zahlungssystemen wie z. B. EC-Karte in Deutschland sein kann.[307]

Die einzelnen Mobile Payment Technologien (z. B. NFC bzw. RFID) wurden bzw. werden in verschiedenen (Pilot-)Projekten eingesetzt und dabei einige Erfahrungen gesammelt, wie dies in vorigen Abschnitten gezeigt wurde.[308] Mobile Payment Systeme befinden sich noch in einem Entwicklungsstadium und haben eine breite Akzeptanz und Nutzung von Zahlungssystemen (zumindest in Deutschland) noch nicht erreicht. Allerdings muss erwähnt werden, dass die regionale Unterschiede in den Zahlungssysteminfrastrukturen und Zahlungskulturen auf der ganzen Welt zu einer unterschiedlichen Akzeptanz und Nutzung der Mobile Payment Systemen geführt haben bzw. führen.[309] Außerdem dürfte es auch sehr wahrscheinlich sein, dass verschiedene Zahlungssysteme für verschiedene Bedürfnisse und Situationen im Leben parallel existieren werden.[310]

Aufgrund noch fehlender Standards der Mobile Payment Systeme besteht ein wirtschaftliches Risiko für die Marktteilnehmer. Jedoch werden hier Konsortien und strategische Allianzen gebildet, um die Standardisierung und Durchsetzung von

---

307 Vgl. o. V. (2009b); o. V. (2010c).

308 Vgl. mit den Erläuterungen und Beispiele im Abschnitt 2.6 Technologien von Mobile Payment Systemen, S. 30 sowie im Abschnitt 2.7 Anwendungsbereiche von Mobile Payments, S. 41.

309 Vgl. mit den Erläuterungen und Beispiele im Abschnitt 2.1 Innovationen und Trends im Bereich „Mobile“, S. 12 und im Abschnitt 2.3 Stellenwert von Mobile Payment im M-Commerce, S. 22 sowie im Abschnitt 2.7 Anwendungsbereiche von Mobile Payments, S. 41.

310 Vgl. mit den Erläuterungen und Beispiele im Abschnitt 2.1 Innovationen und Trends im Bereich „Mobile“, S. 12 und im Abschnitt 2.4 Mobile Payment Typen, S. 23 sowie im Abschnitt 2.7 Anwendungsbereiche von Mobile Payments, S. 41.

Mobile Payment Systemen voranzutreiben und Kosten zu sparen.[311] Zudem müssen die beteiligten Geschäftspartner im Mobile Payment System eindeutig identifizierbar sein, um eigene Gefahren und Risiken zu minimieren. Dies geht jedoch zu Lasten der Anonymität der User, die in ihren Einkäufen und Geschäften anonym bleiben und ihre wahre Identität nicht preisgeben möchten. Um diese bestehenden Konflikte beseitigen bzw. mildern zu können, müssen Lösungsansätze und Konzepte im Spannungsfeld der Sicherheit und Einfachheit, sowie der Identifikation und Anonymität entwickelt werden. Ein solcher Lösungsansatz zu bestehenden Konflikten insbesondere zwischen der Identität und Anonymität wird in den nächsten Kapiteln ausgeführt.

[311] Vgl. mit dem Abschnitt 2.8 Mobile Payment Initiativen, S. 49.

4 Grundlagen der Anonymität

Bisher wurden das Ökosystem und die einzelnen Elemente der Mobile Payment Systeme erläutert. In diesem Kapitel werden nun die Grundlagen der Anonymität für das bessere Verständnis der Problematik geschaffen. Hierfür werden zunächst die Schutzziele der Informations- und Kommunikationssysteme erklärt, um das Thema Anonymität einzuordnen. Danach erfolgt die Begriffsdefinition der Anonymität als eines der Schutzziele der Informationssicherheit. Der Begriff Anonymität wird dabei aus der Sicht der Informatik und der gesetzlichen Regelungen definiert. Dann werden die einzelnen Formen der Anonymität der User in den Informations- und Kommunikationssystemen erklärt. Anschließend werden der Begriff Identität und die verschiedenen Grade der Anonymität erläutert. Im nächsten Abschnitt erfolgt eine allgemeine Bewertung der Anonymität. Dabei werden Pros und Contras der User-Anonymität erläutert. Danach wird die User-Anonymität in stationären und mobilen Kommunikationsnetzwerken behandelt. Im letzten Abschnitt dieses Kapitels wird die Bedeutung der User-Anonymität in Mobile Payment Systemen erklärt.

4.1 Schutzziele der Informations- und Kommunikationssysteme

Die IT-Sicherheit bei offenen Kommunikationsnetzwerken hat höchste Priorität für die beteiligten Personen und Institutionen. Die IT-Sicherheit umfasst die folgenden Bereiche:

- Informationsschutz: Es handelt sich um den Schutz der Daten und Informationen in den IT-Systemen.
- IT-System-Schutz: Darunter wird der Sicherheit und Schutzvorkehrungen der IT-Systeme verstanden.
- IT-System-Normen: Diese beschreiben rechtlichen Schutz der IT-Systeme bzw. die Einhaltung gesetzlicher Regeln und Normen für die IT-Systeme.

Darüber hinaus soll die IT-Sicherheit bestimmte Anforderungen von beteiligten Parteien erfüllen. Im Rahmen der IT-Sicherheit gibt es drei Grundwerte, die Sicherheitsanforderungen der Informations- und Kommunikationssysteme erfüllen sollen:[312]

[312] Vgl. Hansen/Meissner (2007), S. 63ff.; BSI (2006); BSI (2007), S. 8.

1. Vertraulichkeit,

2. Integrität und,

3. Verfügbarkeit

Diese Grundwerte bzw. Schutzziele der Informations- und Kommunikationssysteme können wie folgt erklärt werden:[313]

1. Vertraulichkeit von Informationen und Nachrichten bezeichnet, dass niemand außer dem Absender und dem Empfänger einer Nachricht deren Inhalt kennt. Deshalb sollen unbefugter Informationsgewinn aus dem System und unbefugte Einsichtnahme der Systeminformation oder unberechtigter Zugriff auf Systeminformation verhindert werden, d. h. vertrauliche Informationen sind nur Berechtigten bekannt und sollen nicht von Dritten ausgeforscht werden können. Die Schutzziele der Vertraulichkeit sind:[314]

- **Anonymität** bedeutet, dass der Absender bzw. Empfänger einer Nachricht innerhalb einer Menge möglicher Absender bzw. Empfänger nicht identifizierbar sind. Die User können bestimmte Anwendungen benutzen und Dienstleistungen von Dritten in Anspruch nehmen, ohne dass sie ihre Identität offenbaren müssen. Auch Kommunikationspartner erfahren die Identität des Gegenübers nicht.[315]

- **Unbeobachtbarkeit** des Absenders oder des Empfängers einer Nachricht stellt dar, dass jemand Absender oder Empfänger der Nachricht sein kann, ohne andere außer ihm dies bemerken zu können.

- **Unverkettbarkeit** von Nachrichten und Transaktionen drückt aus, dass Nachrichten und Transaktionen nicht miteinander verknüpft und somit inhaltlich nicht verfälscht werden können.

---

313 Vgl. BSI (2006), S. 45ff. sowie mit den Erläuterungen im Abschnitt 3.2.2.1 Sicherheitsanforderungen, S. 66 und im Abschnitt 3.2.2.2 Integrations- und Realisierungsanforderungen, S. 68.

314 Vgl. Hansen/Meissner (2007), S. 63.

315 Die Definition des Begriffes „Anonymität“ und weitere Erläuterungen über die Anonymität erfolgen im Abschnitt 4.2.1 Begriffsdefinition der Anonymität, S. 85 und in den folgenden Abschnitten im Kapitel 4 Grundlagen der Anonymität.

- **Verdecktheit** des Inhalts einer Nachricht heißt, dass niemand außer dem Absender und dem Empfänger einer Nachricht deren Existenz bemerkt.

2. Integrität von Informationen und Nachrichten bezeichnet, dass Veränderungen von Informationen im System durch Unbefugte verhindert werden sollen, d.h. Informationen sollen unverfälscht und vollständig übertragen werden. Die Schutzziele der Integrität sind:[316]

- **Integrität** des Kommunikationsinhalts und der Kommunikationsumstände einer Nachricht erläutert, dass niemand eine Nachricht nach deren Absenden unbemerkt verändern kann.

- **Zurechenbarkeit** des Absenders bzw. des Empfänger einer Nachricht zeigt, dass ein Absender bzw. Empfänger nicht erfolgreich behaupten kann, eine Nachricht mit diesem Inhalt und den übermittelten Kommunikationsumständen gesendet bzw. erhalten zu haben oder auch nicht gesendet bzw. nicht erhalten zu haben.

- **Datenkonsistenz** des Inhalts und des Absenders einer Nachricht bedeutet, dass alle Empfänger einer Nachricht die gleiche Nachricht mit dem gleichen Inhalt und den gleichen Kommunikationsumständen erhalten oder erkennen können.

3. Verfügbarkeit von Informationssystemen beschreibt, dass eine Beeinträchtigung der Funktionalität des Systems durch Unbefugte verhindert werden soll, d.h. die Funktionen und Services von Systemen und Informationen sollen zum geforderten Zeitpunkt und im vorgegebenen Zeitrahmen unterbrechungsfrei bereitgestellt werden. Die Schutzziele der Verfügbarkeit sind:[317]

- **Verfügbarkeit** des Systems, das die Nachricht vermittelt, beschildert, dass eine Entität[318] eine Nachricht senden oder empfangen kann, wenn sie dies möchte.

---

316 Vgl. Ebenda.

317 Vgl. Hansen/Meissner (2007), S. 63 und 64.

318 Eine Entität ist ein individuelles, unterscheidbares und identifizierbares Exemplar von Dingen, Personen oder Begriffen der realen oder der Vorstellungswelt. Vgl. Moos (2004), S. 11. Eine ähnliche Definition der Entität liefern auch Matthiessen und Unterstein: Eine Entität ist eine eigenständige Einheit, die im Rahmen des betrachteten Modells eindeutig identifiziert werden kann.

Fortsetzung auf der nächsten Seite

- **Erreichbarkeit** der Entitäten innerhalb des Systems kennzeichnet, dass Entitäten über eine Nachricht - abhängig von deren Wünschen - erreicht werden können oder auch nicht.

- **Fairness** der Entitäten untereinander besagt, dass alle Absender bzw. Adressaten die gleichen Möglichkeiten zum Senden bzw. Empfangen einer Nachricht haben.

- **Verbindlichkeit** der Entitäten bedeutet, dass Entitäten dafür verantwortlich gemacht werden können, versprochenen Verpflichtungen (Rechtsverbindlichkeit) nachzukommen.

- **Authentizität** bezeichnet die eindeutige Abbildung realer Identität des Absenders auf digitale Identität. Die Authentizität bildet die Grundlage für Autorisierung, Anonymität und Abrechnung.

Problematisch bleiben die Schutzziele Anonymität und Authentizität, da die beiden Schutzziele in digitalen Netzwerken miteinander in Konkurrenz stehen. Die Möglichkeit einer sicheren Identifikation von Personen (Authentizität) bringt den Verlust der Geheimhaltung der Identität (Anonymität) mit sich. In diesem Fall muss je nach Anwendung bzw. Prozess gegenüberstellt und beurteilt werden, welche von beiden Schutzzielen zweckmäßig ist und bevorzugt werden soll. Der User soll dann die Möglichkeit erhalten, zwischen den beiden Schutzzielen wählen zu können.[319]

4.2 Anonymität als Schutzziel der Informationssicherheit

Bei der Informationssicherheit geht es um den Schutz vor Gefahren und Bedrohungen sowie die Vermeidung von Schäden und die Minimierung von Risiken für Informationssysteme. Beim Datenschutz geht es hauptsächlich um den Schutz personenbezogener Daten vor Manipulation bzw. Missbrauch. Personenbezogene Daten beschreiben persönliche oder sachliche Verhältnisse einer natürlichen Person. Es ist hinreichend, auch wenn die Person namentlich unbekannt, jedoch durch z.B. Personalnummer, Telefonnummer, E-Mail-Adresse oder IP-Adresse bestimmbar ist. Insbesondere findet der Schutz personenbezogener Daten seinen Ausdruck in der

---

Eine Identität kann z. B. ein Gegenstand, eine Kategorie von Gegenständen, eine Person, ein Ereignis, eine abstrakte Größe oder ein Dokument sein. Vgl. Matthiessen/Unterstein (2003), S. 92.

[319] Vgl. BSI (2006), S. 15, 46 und 67.

informationellen Selbstbestimmung. Danach kann jeder einzelne prinzipiell selbst entscheiden, was mit seinen personenbezogenen Daten geschieht bzw. geschehen soll. Hier wird die Privatsphäre von der öffentlichen Sphäre getrennt und geschützt. Der Umgang mit personenbezogenen Daten ist im Grundgesetz und in verschiedenen Datenschutzgesetzen wie Bundesdatenschutzgesetz zusammen mit den Datenschutzgesetzen der Länder geregelt.[320] Dabei gibt es verschiedene bereichspezifische Datenschutzbestimmungen wie Sozialgeheimnis, Steuergeheimnis, Postgeheimnis und Schweigepflicht etc.

4.2.1 Begriffsdefinition der Anonymität

In den vorhandenen Quellen wird der Begriff „Anonymität“ unterschiedlich definiert. Aus diesem Grund werden zunächst die bereits existierenden Definitionen der Anonymität und deren Unterschiede gezeigt werden. Erste Definitionen des Begriffs „Anonymität“ finden sich in den Online-Literaturquellen unter der Wikipedia. Unter der Wikipedia-Seite in deutscher Sprache ist die folgende Definition der Anonymität zu finden:

„*Anonymität ist die Geheimhaltung der Identität einer Person, einer Gruppe, einer Institution oder einer agierenden Struktur.*“[321]

Wobei sich die Definition explizit auf eine Person, eine Personengruppe und eine Organisation bezieht.

Unter der Wikipedia-Seite in englischer Sprache ist die folgende Definition der Anonymität zu finden:

„*Anonymity is derived from the Greek word ανωνυμία, meaning "without a name" or "namelessness". In colloquial use, the term typically refers to a person, and often means that the personal identity or personally identifiable information of that person is not known.*”[322]

„*More strictly, and in reference to an arbitrary element (e.g. a human, an object, a computer), within a well-defined set (called the "anonymity set"), "anonymity" of that*

---

[320] Vgl. BDSG im Internet http://bundesrecht.juris.de/bdsg_1990/, Stand: 31.05.2009.

[321] Vgl. Wikipedia (2010a).

[322] Vgl. Wikipedia (2010b).

element refers to the property of that element of not being identifiable within this set. If it is not identifiable, then the element is said to be "anonymous"."[323]

Auch in dieser Definition bezieht sich die Anonymität in erster Linie auf eine Person und deren Identität und Nicht-Identifizierbarkeit, wobei in der Begriffsdefinition zusätzlich auch von Sachen und Objekten die Rede ist.

In der Wissenschaftsliteratur werden folgende Begriffsdefinitionen der Anonymität verwendet:

Beutelspacher definiert den Begriff „Anonymität" im Zusammenhang mit der Kryptologie[324]:

„*Üblicherweise assoziiert man mit „Geheimhaltung" die Geheimhaltung von Nachrichten. In vielen Situationen ist aber auch gewünscht, dass die am Nachrichtenaustausch beteiligten Instanzen geheim bleiben. In diesem Fall spricht man von Anonymität*"[325]

Dannenberg und Ulrich definieren den Begriff „Anonymität" im Zusammenhang mit E-Commerce und E-Payment:

„*Allgemein spricht man von Anonymität in dem Sinne, dass die Identität einer Person nicht bekannt ist; sie ist namenlos. Anonyme Zahlungstransaktionen sind dann jene, bei denen die Identität des Zahlenden verborgen bleibt. Möglich sind solche Transaktionen mit Bargeld*."[326]

Pfitzmann und Hansen verwenden die folgende Definition des Begriffs „Anonymität":

„*Anonymity of a subject means that the subject is not identifiable within a set of subjects, the anonymity set* "[327]

---

[323] Vgl. Ebenda.

[324] Kryptologie befasst sich mit der Übertragung von Nachrichten, die solcherart codiert sind, dass ein unbefugter Abhörer eines solchen Codes möglichst nicht auf die eigentliche Nachricht rückschliessen kann. … Hierbei umfasst die Wissenschaft der Kryptologie sowohl die Kryptographie (wie man Nachrichten geeignet verschlüsselt), als auch die Kryptoanalyse (welche Methoden man aus der Sicht des unberechtigten Abhörers einsetzen kann, um evtl. doch an die Nachricht heranzukommen). Vgl. Schöning (2006), 219.

[325] Vgl. Beutelspacher (2007), S. 129.

[326] Vgl. Dannenberg/Ulrich (2004), S. 54.

[327] Vgl. Pfitzmann/Hansen (2009), S. 9.

"*… we regard a subject as a possibly acting entity such as, e.g., a human being (i.e. a natural person), a legal person, or a computer.*"[328]

Nach der Definition von Pfitzmann und Hansen wird unter Anonymität als „*der Zustand innerhalb einer Menge von Subjekten nicht identifizierbar zu sein"* verstanden. Die Menge von Subjekten wird als Anonymitätsmenge bezeichnet. Die Größe der Anonymitätsmenge bestimmt den Grad der Anonymität von Subjekten. Eine weitere Begriffsdefinition liefern Köpsell und Pfitzmann und betrachten die Anonymität aus der Perspektive des Verhaltens einer Person und Gruppe. Danach:

„Anonymität bezeichnet dabei den Zustand, nicht unterscheidbar innerhalb einer Gruppe zu sein, die sich ähnlich (gleich) verhält. Einfach gesagt gilt, dass je mehr Mitglieder diese Gruppe hat und je ähnlicher das Verhalten der Mitglieder ist, desto größer ist die Anonymität. Man ist also, wenn man anonym sein will, auf die Mithilfe anderer angewiesen."[329]

In dieser Definition ist die Rede nicht nur von einer Person und deren Identität, sondern auch von ihrem Verhalten. Folglich wird in einer Definition der Anonymität von der Anonymitätsmenge (Anonymity Set), der Unbeobachtbarkeit (Unobservability) und der Unverkettbarkeit (Unlinkability) gesprochen. In der bisherigen Anonymitätsforschung ist die Anonymitätsmenge als die Menge der Identitäten möglicher Absender und Empfänger definiert. Ein wichtiger Aspekt der Anonymität ist die Unbeobachtbarkeit. Die Unbeobachtbarkeit beschreibt die Eigenschaft, dass die Übertragung der Nachrichten unsichtbar für die Beobachter oder Angreifer ist. Außerdem wird die Anonymität hinsichtlich der Unverkettbarkeit definiert. Die Unverkettbarkeit beschreibt die Eigenschaft, dass der Absender oder Empfänger einer Nachricht innerhalb einer anonymen Gruppe bzw. deren Beziehung miteinander nicht identifizierbar ist.

4.2.2 Legaldefinition der Anonymisierung

Der Begriff „Anonymität" wird im Gesetz im Zusammenhang mit der Anonymisierung personenbezogener Daten definiert. Dies zeigt die Konkretisierung des Begriffs Anonymität in den Sachverhalten, wird daher von der Anonymisierung, also der

---

328 Vgl. Ebenda, S. 7.

329 Vgl. Köpsell/Pfitzmann (2003), S. 5.

Geheimhaltung der personenbezogenen Daten im Gesetz gesprochen. Der Gesetzgeber definiert den Begriff „Anonymisierung“ in § 3 Abs. 6 BDSG wie folgt:[330]

„Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.“

Aus diesen verschiedenen Definitionen und Ausführungen für den Begriff kann eine zusammenfassende Definition abgeleitet werden. Danach kann die Anonymität als der Zustand innerhalb einer Menge von Subjekten, die sich ähnlich verhalten, nicht identifizierbar zu sein definiert werden. Darüber hinaus kann die User-Anonymität als der Zustand der Nichtidentifizierbarkeit der natürlichen Personen innerhalb einer Menge von Personen (Usern), die ähnliche Eigenschaften vorweisen, definiert werden, wobei die Einzelinformationen über persönliche und sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Zeit-, Geld- und Arbeitsaufwand einer bestimmten oder bestimmbaren Personen zugeordnet werden können.

Zusammenfassend kann festgehalten werden, dass die drei Elemente der Begriffsdefinition der Anonymität (Anonymitätsmenge, Unbeobachtbarkeit und Unverkettbarkeit) sowie die legale Definition der Anonymisierung für die Beschreibung und Gestaltung der User-Anonymität sehr relevant sind.

4.3 Formen der Anonymität

In diesem Abschnitt wird erklärt, welche Formen der Anonymität in den Kommunikationsnetzwerken wie z. B. Internet existieren, was deren Umfang ist und welche Unterschiede zwischen den Formen der Anonymität bestehen. Die Form der Anonymität in den Kommunikationsnetzen wird durch die verschiedene Faktoren und Umständen bestimmt, die wie folgt dargestellt werden können:[331]

---

[330] Vgl. BDSG § 3 Weitere Begriffsbestimmungen, http://bundesrecht.juris.de/bdsg_1990/__3.html, Stand: 16.10.2009.

[331] Vgl. Federrath/Pfitzmann (1998), S. 628.

- Durch das Senden einer Nachricht: Hierdurch kann die Identität bzw. Anonymität eines Senders festgestellt werden. Hier ist das Senden einer Nachricht entscheidend für die Anonymitätsform.

- Durch das Empfangen einer Nachricht: Die Anonymitätsform wird durch das Empfangen einer Nachricht bestimmt. Das heißt, durch das Empfangen einer Nachricht kann die Identität bzw. Anonymität eines Empfängers bestimmt werden. Hier ist der Empfänger einer Nachricht ausschlaggebend für die Anonymitätsform.

- Durch eine Kommunikationsbeziehung zwischen zwei oder mehr Instanzen (z.B. Personen oder Server): Die Identität bzw. Anonymität der Kommunikationsbeteiligten und der Kommunikationsinhalt kann in einer Kommunikation bestimmt werden. Die Kommunikationsbeziehung ist entscheidend für die Anonymitätsform.

- Durch den Standort bzw. Aufenthaltsort der beteiligten Instanzen: Die Identität bzw. Anonymität der beteiligten Instanzen (Personen oder Server) können durch ihre Standorte bzw. Aufenthaltsorte bestimmt werden.

- Durch den Zeitpunkt der Kommunikation: Ebenfalls kann durch die Zeitangaben einer Kommunikation die Identität bzw. Anonymität der beteiligten Instanzen bestimmt werden. Gemeint sind der Anfang, das Ende und die Dauer einer Kommunikation.

Die Faktoren und Umstände, die die Form der Anonymität bestimmen, können systematisiert werden. Die Systematik der Anonymitätsformen wird in der Abbildung 11, S. 90 dargestellt. In einem Kommunikationsmodell beschreiben Pfitzman und Waidner drei Anonymitätsformen:[332]

1. Senderanonymität
2. Empfängeranonymität
3. Kommunikationsanonymität

Die Senderanonymität und Empfängeranonymität können unter Prozessanonymität zusammengefasst werden. Die Prozessanonymität wird durch die Kommunikationsprotokolle und deren Kommunikationsschichten bestimmt und kann durch ein

[332] Vgl. Pfitzmann/Waidner (1986), S. 246ff.; Reiter/Rubin (1997), S. 3; Beutelspacher (2007), S. 129; Beutelspacher/Schwenk/Wolfenstetter (2006), S. 79.

Kommunikationssystem automatisch hergestellt werden, wenn dies schon in der Designphase des Kommunikationssystems geplant wurde.[333]

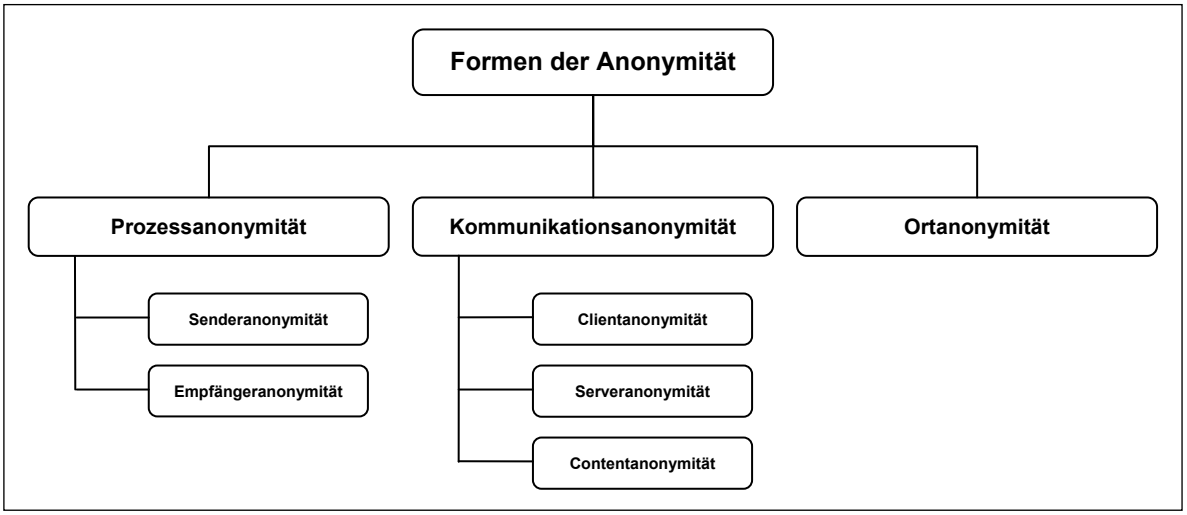

Abbildung 11: Anonymitätsformen in den Kommunikationsnetzwerken

Die Kommunikationsanonymität lässt sich wiederum nochmals in drei Anonymitätsformen unterteilen, da eine Kommunikation zwischen verschiedenen Instanzen, also nicht nur Personen, sondern auch Maschinen (Server) stattfindet. Demuth und Rieke unterscheiden zunächst zwischen der Client- und Serveranonymität in einer Kommunikationsbeziehung.[334] Zudem erklären Kobsa und Schreck in ihrem Forschungsbeitrag die Contentanonymität in einer Kommunikationsbeziehung.[335] Die Kommunikationsanonymität unterteilt sich wie folgt in drei Formen:

- Clientanonymität[336]

---

333 Vgl. Kobsa/Schreck (2003), S. 157.

334 Vgl. Demuth/Rieke (1998), S. 623.

335 Vgl. Kobsa/Schreck (2003), S. 157.

336 Client ist die englische Bezeichnung für „Klient“, „Mandant“ und wird ein Computerprogramm bezeichnet, welches nach dem Client-Server-System Verbindung mit einem Server aufnimmt und Nachrichten mit diesem austauscht. Die Kommunikation erfolgt vorwiegend über ein Rechnernetz. Das heißt, der Server befindet sich normalerweise auf einem anderen Rechner als der Client. Ein typisches Beispiel für einen Client ist ein Web-Browser. Dieser nimmt Kontakt zu einem Web-Server auf und fordert eine bestimmte Webseite von diesem an. Der Server schickt die angeforderte Webseite zu, damit dieser sie dann für den User in einem Browserfenster anzeigt. Als Clients bezeichnet man auch die Computer in einem Rechnernetz, die auf einen bestimmten Server zugreifen. Ebenso werden in einem drahtlosen Netz die Netzwerkkomponenten oder Rechner, die vom Access Point (Schnittstelle für drahtlose Kommunikationsgeräte) versorgt werden, als Clients bezeichnet. Vgl. Maffeis (1997), S.1ff., Stand: 29.01.2010.

- Serveranonymität
- Contentanonymität.

Diese Teilung kann aufgrund der Mobilität der User, der mobilen Kommunikation mit dem Faktor Ort ergänzt werden. Somit kann von einer Ortanonymität gesprochen werden, da der mobile User in einer mobilen Kommunikation seinen Stand- bzw. Aufenthaltsort ändert.

- Ortanonymität

Im Folgenden werden die hier kurz dargestellten Formen der Anonymität detailliert erklärt.

4.3.1 Prozessanonymität

4.3.1.1 Senderanonymität

Die Senderanonymität bedeutet, dass das Verschicken einer Nachricht anonym erfolgt und der User als Sender unerkannt bleibt, wenn er nicht durch den Empfänger innerhalb einer Menge potentieller Sender identifiziert werden kann.[337] Ein Beobachter kann nicht feststellen, wer diese Nachricht gesendet hat. Die Zuordnung einer Nachricht zu einem Sender ist nicht möglich oder nur mit erheblichem Aufwand zu realisieren. Auf der anderen Seite kann die Identität des Empfängers oder die Nachricht selbst in dieser Kommunikationsbeziehung bekannt sein.[338] Die Senderanonymität wird in der Abbildung 12, S. 92 graphisch dargestellt. Diese Anonymitätsform kommt beispielsweise im Internet zur Anwendung. Wenn der User im Internet surft, sendet er Anfragen an den Zielwebserver über einen Anonymisierungsdienst, um anonym zu bleiben. Der Anonymisierungsdienst verheimlicht die wahre IP-Adresse des Users. Somit kann der Zielwebserver nicht feststellen, woher die Anfragen stammen und keine Rückschlüsse auf die Identität des Users ziehen. Die Senderanonymität wird im Abschnitt 5.2.4 Anonymitätskonzepte, S. 124 mit Praxisbeispielen näher erklärt.

---

[337] Vgl. Pfitzmann/Waidner (1986), S. 246ff; Reiter/Rubin (1997), S. 3; BSI (2001); Kobsa/Schreck (2003), S. 157.

[338] Vgl. Ebenda.

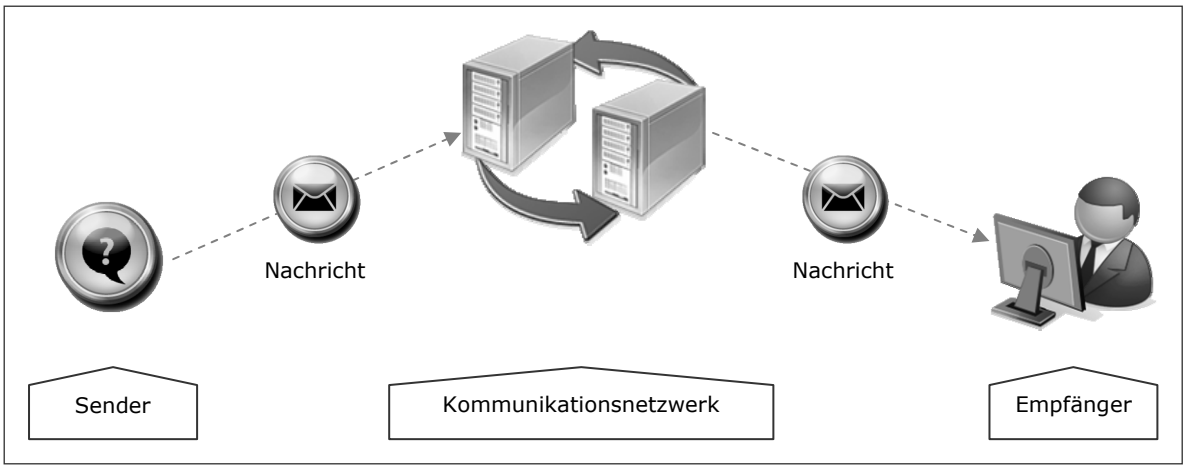

Abbildung 12: Senderanonymität[339]

4.3.1.2 Empfängeranonymität

Die Empfängeranonymität bedeutet, dass die Identität des Empfängers für den Sender der Nachricht unbekannt ist.[340] Bei der Empfängeranonymität kann der User als Empfänger einer Nachricht seine Identität gegenüber dem Sender verbergen. Ein Beobachter kann nicht feststellen, wer eine Nachricht empfangen hat. Die Empfängeranonymität spielt eine wichtige Rolle bei der Beantwortung der Nachrichten zu einem anonymen Empfänger, die schon unter der Senderanonymität empfangen wurden. Die Empfängeranonymität wird in der Abbildung 13, S. 93 graphisch dargestellt. Sie kann beispielsweise durch „Broadcasting“ erreicht werden; Dabei wird die Nachricht an alle Instanzen gesendet, obwohl sie nur für eine bestimmte Instanz bestimmt ist.[341] Die Broadcastmedien Rundfunk und Fernsehen sind Beispiele für die Empfängeranonymität.[342]

---

339 In Anlehnung an BSI (2001).

340 Vgl. Pfitzmann/Waidner (1986), S. 246ff; Reiter/Rubin (1997), S. 3; BSI (2001); Kobsa/Schreck (2003), S. 157.

341 Vgl. Beutelspacher/Schwenk/Wolfenstetter (2006), S. 79.

342 Vgl. Pfitzmann/Waidner (1986), S. 246; Beutelspacher (2007), S. 132.

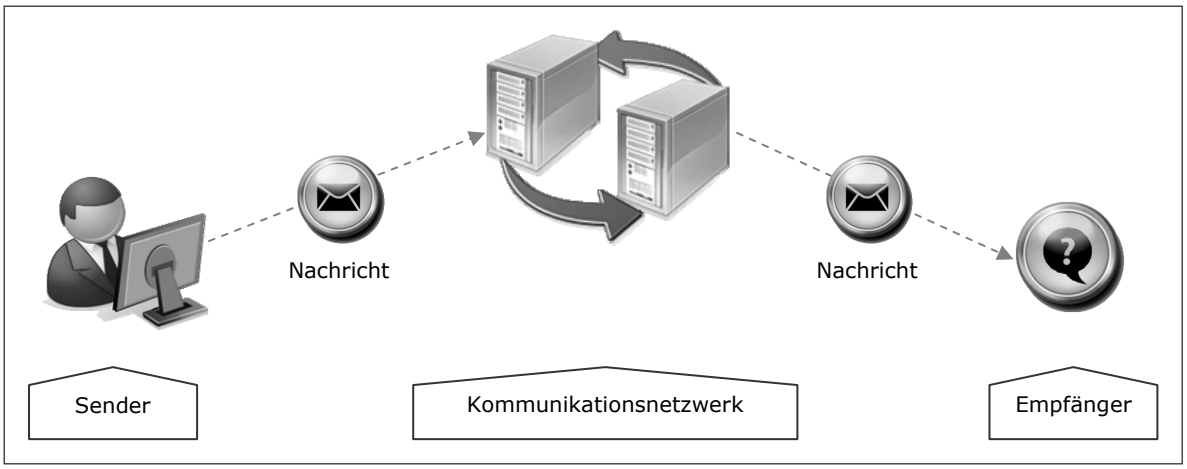

Abbildung 13: Empfängeranonymität[343]

4.3.2 Kommunikationsanonymität

Neben den beteiligten Instanzen (Personen und Server) spielt auch die Anonymität der Kommunikationsbeziehung eine wichtige Rolle. In einer anonymen Kommunikation bleiben sowohl Sender und Empfänger voreinander anonym, als auch die Kommunikationsbeziehung zwischen ihnen bleibt verborgen. Ein Beobachter innerhalb oder außerhalb des Systems kann nicht feststellen, welche Nachricht von welchem Sender stammt und von wem diese empfangen wird. Das heißt, ein Beobachter im Kommunikationsnetz kann zwar erkennen, dass ein User eine Nachricht einem anderen sendet und ein anderer User eine Nachricht von einem anderen empfängt. Er kann aber nicht eindeutig feststellen, dass die zwei User miteinander kommunizieren, da auch andere User miteinander in einem Kommunikationsnetzwerk gleichzeitig kommunizieren. Das Anonymitätskonzept der Mixe bietet diese Möglichkeit und wird später im nächsten Kapitel näher erklärt werden.[344] Die Kommunikationsanonymität wird in der Abbildung 14, S. 94 graphisch dargestellt.

[343] In Anlehnung an BSI (2001).

[344] Vgl. mit dem Abschnitt 5.2.4.4 Mixe und deren Anwendung in der Praxis, S. 133.

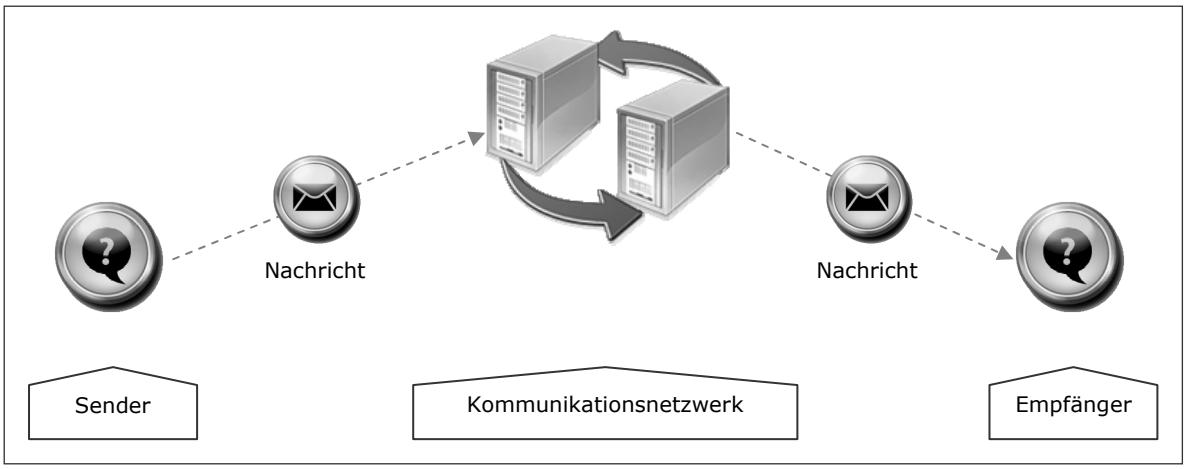

Abbildung 14: Kommunikationsanonymität[345]

Neben den erwähnten Anonymitätsformen in einem Kommunikationsmodell erklären Demuth und Rieke in einer Client-Server-Kommunikationsbeziehung die Client-Anonymität und Server-Anonymität. Danach nutzen User (Clients) über die Kommunikationsprotokolle Dienstleistungen von Service Providern (Servers).[346] Dabei benutzen User Webbrowser wie Internet Explorer, Mozilla Firefox oder Opera, um Webseiten abzurufen. Webbrowser (Client) und Webserver kommunizieren miteinander über die Hypertext Transfer Protocol (HTTP). Jede Webseite hat eine URL-Adresse, mit der die Webseite weltweit zu lokalisieren ist.[347] Wenn der User (Client) eine Webseite abruft, sendet der Webbrowser an den Webserver eine HTTP-Anfrage mit der URL-Adresse und den Metadaten. Der Webserver sendet eine Antwort mit dem Webseiteninhalt und den Metadaten zurück.[348]

4.3.2.1 Client-Anonymität

In einer Client-Server-Kommunikationsbeziehung kommunizieren die User und Service Provider über Netzwerkprotokolle miteinander. In dieser Kommunikationsbeziehung nutzt der User mit einem Webbrowser die Dienstleistungen von Service Provider. Beim Abruf einer Webseite werden, wie bereits erwähnt, die Metadaten über den Webbrowser und die Konfiguration des Rechners vom User an den Web-

345 In Anlehnung an BSI (2001).

346 Vgl. Demuth/Rieke (1998), S. 623.

347 Vgl. Gourley et al. (2002), S. 23.

348 Metadaten sind Informationen über andere Daten und enthalten Angaben über die Eigenschaften eines Objektes. Vgl. http://www2.sub.uni-goettingen.de/intrometa.html sowie http://www.w3.org/Metadata/, Stand: 18.01.2010.

server übermittelt. Diese Metadaten enthalten in der Regel verschiedene Informationen über den Computer und Browser des Users. Dabei werden normalerweise folgende Daten und Informationen mit dem Abruf einer Webseite an den kontaktierten Webserver übermittelt:[349]

- Typ und Version des Betriebssystems (Windows, Linux oder Mac etc.)
- Numerische Internet-Adresse des Computers (IP-Adresse wie 134.96.6.1)
- Symbolische Adresse (www.uni-kassel.de)
- Ort des Internet-Zugangs
- Typ und Version des Webbrowsers
- URL-Adresse der zuvor besuchten Webseite
- Kontakthäufigkeit eines Webservers via Cookies
- E-Mail-Adresse und Typ und Version des benutzten E-Mail-Programms

Mit diesen übermittelten Metadaten erhalten Betreiber des kontaktierten Webservers eine Reihe von Daten und Informationen über die User, ohne dass diese es wissen bzw. merken. Die Betreiber des kontaktierten Webservers haben somit die Möglichkeit, Daten und Informationen über die User zu sammeln, diese zu bewerten und potentiell diese auch zu manipulieren. So haben beispielsweise die Betreiber der Webserver folgende Möglichkeiten mit den gesammelten Daten und Informationen:[350]

- Analyse von Webnutzungsverhalten
- Erstellung von Userprofilen und -statistiken
- Untersuchung persönlicher Vorlieben
- Handel mit den Userdaten wie z. B. Verkauf von E-Mail-Adressen[351]

---

349 Vgl. Demuth/Rieke (1998), S. 623.

350 Vgl. Ebenda.

351 Mehr Infos über Handel mit E-Mail-Adressen unter http://www.chip.de/news/Illegaler-Handel-mit-E-Mail-Adressen-blueht_34204608.html, Stand: 21.06.2009.

- Nutzung von Userdaten für Werbe- und Marketing-Zwecke
- Austausch und Abgleich von Userprofilen und Nutzungsverhalten durch Kooperation von Betreibern der Webserver

Wenn ein User seine Identität gegenüber den Betreibern von Webservern in einer Client-Server-Kommunikationsbeziehung nicht offenbaren möchte, wird dies Client-Anonymität bezeichnet.[352] Der Client (User) bleibt bezüglich seiner Identität gegenüber dem Server unbekannt und hat die Möglichkeit, seine Identität zu schützen und dadurch im Internet anonym zu surfen. Hierbei werden durch Weglassen und Abändern von Email-Adressen, IP-Adressen, besuchten Seiten, Betriebssystemen, Webbrowsern und regelmäßiges Löschen von Cookies verhindert, dass die Betreiber von Webservern beim Surfen ein Profil von Usern erstellen können.

4.3.2.2 Server-Anonymität

In einer Client-Server-Kommunikationsbeziehung ist auch die Server-Anonymität von großer Bedeutung, wenn der Service Provider oder Anbieter einer Webseite anonym bleiben möchte. Die Anonymität des Serviceanbieters ist aus folgenden Gründen nachvollziehbar:[353]

- Anonyme Befragungen und Anzeigen,
- Anonymes Publizieren von Inhalten bzw. Webseiten,
- etc.

Die Webadresse des Serviceanbieters muss den Usern bekannt bleiben. Diese Webadresse gibt jedoch bereits Auskunft über den Server. So kann der User den Ort und die Herkunft des Webservers anhand der URL ermitteln. Bei der Server-Anonymität haben die Betreiber eines Webservers die Möglichkeit, ihre Identität zu verbergen. Durch RSA-Verfahren werden die Identität von Webservern und Hyperlinks auf der Webseite verschlüsselt.[354] Die User können aber mit dem Server ver-

[352] Vgl. Demuth/Rieke (1998), S. 624.

[353] Vgl. Ebenda.

[354] Das RSA-Verfahren ist ein asymmetrisches Kryptosystem, das sowohl zur Verschlüsselung als auch zur digitalen Signatur verwendet werden kann. Es verwendet ein Schlüsselpaar bestehend aus einem privaten Schlüssel, der zum Entschlüsseln oder Signieren von Daten verwendet wird, und einem öffentlichen Schlüssel, mit dem man verschlüsselt oder Signaturen prüft. Der private

Fortsetzung auf der nächsten Seite

bunden bleiben. Der Server bzw. die Webseite auf dem Server bleibt gegenüber dem Client bezüglich ihres Ortes unbekannt.[355]

4.3.2.3 Contentanonymität

Die Contentanonymität besagt, dass keine Identifizierung durch die ausgetauschten Daten und Informationen in einer Kommunikationsbeziehung möglich ist. Ein Angreifer bzw. Beobachter kennt u. U. den Inhalt der Kommunikation. Die User können in einer Kommunikation identifiziert werden durch:[356]

- den Inhalt (z.B. Name, Adresse, E-Mail-Adressen oder Kombination einzelner Datenwerte),
- die Struktur der Daten (z.B. Darstellung der Daten in einem Formular oder Software) und
- die Reihenfolge der Daten (z.B. sich wiederholende Muster der Daten, durch die getrennte Sitzungen verkettet werden).

Außerdem können mit einem einzigen Merkmal vom User auch andere Merkmale abgeleitet werden.[357]

4.3.3 Ortanonymität

Wenn der User seinen Standort und Aufenthaltsort wechselt, kann ein Dritter (Beobachter oder Angreifer etc.) seine Bewegung anhand der Verkettung der Aufenthaltsorte und Datenverkehr beobachten und daraus Bewegungsmuster erstellen. Die Ortanonymität soll gewährleisten, dass der Standort des Empfängers oder Senders nicht von Dritten nachvollzogen werden kann.

Schlüssel wird geheim gehalten und kann nicht oder nur mit extrem hohem Aufwand aus dem öffentlichen Schlüssel berechnet werden. Vgl. http://www.itwissen.info/definition/lexikon/Rivest-Shamir-Adleman-RSA-RSA-Verfahren.html sowie http://www.rsa.com/node.aspx?id=2760, Stand: 21.06.2009.

355 Nähere Informationen über Server-Anonymität geben Demuth und Rieke im JANUS-Projekt, Vgl. Demuth und Rieke (1998), S. 625.

356 Vgl. Kobsa/Schreck (2003), S. 157.

357 Vgl. Ebenda.

Hinsichtlich des Begriffs „Mobilität“ unterscheiden sich die Begriffe der mobilen Anonymität und der Identitätsanonymität voneinander. In stationären Kommunikationsnetzwerken (z.B. Internet) sind die Identität eines Absenders oder Empfängers und deren Aufenthaltsorte gleich. Die Identität des Absenders oder Empfängers kann durch die IP-Adresse oder einen Domänennamen ermittelt werden. Die Identifizierung der Aufenthaltsorte des Absenders oder Empfängers impliziert auch die Beeinträchtigung der Anonymität vom Absender und Empfänger. Auf der anderen Seite wechseln der Absender und Empfänger in mobilen Netzwerken ihre Aufenthaltsorte ständig. Somit sind der Absender und Empfänger von ihren Aufenthaltsorten getrennt.[358]

Die mobile Anonymität wird auch als Ortanonymität definiert und umfasst den Ereignisort, die Privatsphäre und den Datenschutz sowie den Schutz der Bewegungsmuster mobiler User. Die Ortanonymität (Venue Anonymity) ist die Menge aller Ereignisorte. Danach wird die Ortanonymität als der Zustand der Nichtidentifizierbarkeit der Orte von Absendern und Empfängern innerhalb einer Menge von Ereignisorten definiert. Die Beziehung zwischen dem Ort des Absenders und dem Ort des Empfängers sollte innerhalb einer Menge von Ereignisorten nicht verkettbar sein. Hier wird die Ortanonymität parallel zur konventionellen Identitätsanonymität definiert.[359]

4.4 Identität und Grade der Anonymität

Der User besitzt verschiedene Identitäten entsprechend seinen Rollen und Taten in der Gesellschaft. Diese Identitäten lassen sich in einer Identitätslandkarte, die von Mark Dixon[360] entwickelt wurde, in vier Gruppen klassifizieren:[361]

- Persönliche Identität beschreibt die einzigartigen Attribute und Kriterien wie Name, Charakteristika, Reputation, Erfahrungen etc., die eine Person einmalig besitzt.

---

358 Vgl. Hong/Kong/Gerla (2006), S. 281.

359 Vgl. Ebenda.

360 Mark Dixon ist der Chief Identity Officer, North America Software Line of Business bei Sun Microsystems, http://blogs.sun.com/identity/, Stand: 24.10.2009.

361 Vgl. Ruedin (2009), S. 10ff.; Zischke (2008), Modelle unserer Identität, http://www.dialogus.de/magazin/ideen/99, Stand: 24.10.2009.

- Physische Identität beschildert die harten Tatsachen wie Geburts- und Heiratsurkunde, Personalausweis, Führerschein, Zeugnis und Diplom etc., die eine Person dokumentarisch besitzt.

- Digitale und virtuelle Identität beinhaltet die Elemente wie Benutzername, Benutzer-ID, Pseudonyme etc., die eine Person oder Sache in der digitalen Welt darstellt, wobei die digitale Identität meist nur einzelne Teile einer gesamten Personenidentität umfasst. Die digitale Identität hilft hauptsächlich ein Vertrauen zwischen den Menschen und Systemen in der virtuellen Welt zu bilden.

- Multiple Identität bildet sich aus den physischen und digitalen Komponenten der Identität wie SmartCard, Kreditkarte, Krankenkassenkarte, elektronische Zugangskarten etc.

In einem anderen Modell, das von Andre Durand[362] entwickelt wurde, der speziell die Struktur einer digitalen Identität analysiert hat, wird das Verhältnis zwischen einer Person, Unternehmen und Aggregation von Daten betrachtet.[363] Das 3-Ebenen-Identitäts-Model wird in der Abbildung 15, S. 100 dargestellt und beinhaltet folgende Ebenen:

- Auf der Ebene 1 wird die persönliche (Ich-) Identität dargestellt und impliziert die reale und persönliche digitale Identität einer Person, die zeitlos und unabhängig von bestimmten Bedingungen ist und durch die Person bestimmt wird.[364]

- Auf der Ebene 2 befindet sich die Unternehmen-(Wir-)Identität, die den Usern zugewiesen wird und nicht zwingend dokumentarisch ist. Diese Identität kann zeitlich begrenzt und von bestimmten Bedingungen abhängig sein. Beispiele sind die Telefon- oder Kontonummer, die den Usern von der Telekom oder Bank zugewiesen wird.[365]

- Auf der Ebene 3 ist die Marketing-(Sie-)Identität. Diese Identität ist eine aggregierte Identität, die aus den demografischen Daten und Informationen

[362] Ausführliche Informationen über Andre Durand unter http://blog.andredurand.com/?p=22, Stand: 24.10.2009.
[363] Vgl. Ruedin (2009), S. 11; Zischke (2008).
[364] Vgl. Zischke (2008).
[365] Vgl. Ebenda.

der Reputation einer Person besteht. Diese Identität wird für die Marketingzwecke von Unternehmen verwendet. Außerdem wird diese Identität von staatlichen Institutionen verwendet. Die Aggregation von Daten- und Informationen machen verschiedene Analysen und Aktionen möglich.[366]

Zischke führt außerdem aus, dass die Identität der Marken, Unternehmen und Personen sowohl durch das Bild des Senders, als auch des Empfängers geformt wird. Danach ist die Identität nicht nur ein Ergebnis der originären Merkmale, sondern kann auch bewusst und gezielt gestaltet werden.[367] Die Bedeutung der verschiedenen Identitäten, insbesondere der digitalen Identität, erwähnen Ruedin und Szugat et al. in sog. Social Software, Web 2.0 und Sozialen Netzwerken. Danach konnte die Social Software erst durch die Gestaltungsmöglichkeiten der digitalen Identität und die Bereitschaft der User, selbst Webinhalte (User generated content) zu schaffen, und die Bereitschaft, ihre Anonymität im Netz teilweise oder ganz aufzugeben, entstehen und ihre Erfolge feiern. [368]

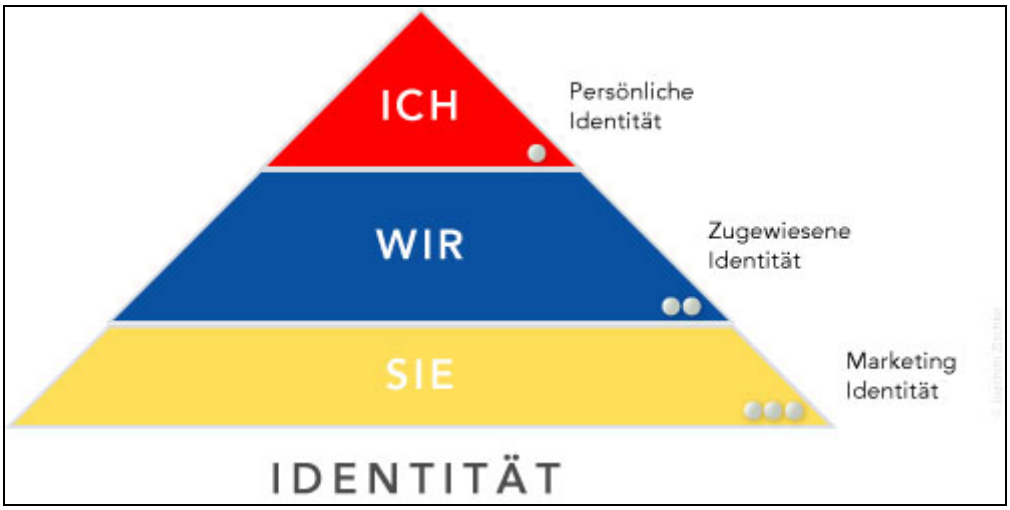

Abbildung 15: 3-Ebenen-Identitäts-Modell von Andre Durand[369]

Das Unterscheidungskriterium für den Grad der Anonymität ist die Identität und Identifizierbarkeit des jeweiligen Kommunikations- bzw. Transaktionspartners. Das heißt, in wie weit kennen die Personen bzw. Instanzen ihre Kommunikations- und Transaktionspartner und ob derjenige Kommunikations- und Transaktionspartner

366 Vgl. Ebenda.

367 Vgl. Zischke (2008).

368 Vgl. Ruedin (2009), S. 11; Szugat/Gewehr/Lochmann (2006), S. 14.

369 Vgl. Ausführliche Informationen über das Modell und Andre Durand unter http://blog.andredurand.com/?p=146, Stand: 24.10.2009.

identifizierbar ist bzw. dessen Identität aufgedeckt werden kann.[370] Danach lässt sich der Grad der Anonymität nach der Bekanntheit der beteiligten Parteien und Instanzen (Personen oder Server) in einer Transaktion klassifizieren.[371] Es gibt verschiedene Grade der Anonymität der Transaktionsparteien und -instanzen (Nachfrager oder Anbieter sowie Sender oder Empfänger). Außerdem können die verschiedenen Grade der Anonymität als ein Kontinuum im Spannungsfeld der absoluten Identität und der absoluten Anonymität wie in der Abbildung 16 dargestellt, gezeigt werden. Spann et al. führt aus, dass zwischen den Extremfällen „Absolute Anonymität“ und „Vollständige Aufdeckung“ mehrere Zwischenstufen wie Pseudonymität und Aggregation möglich sind.[372] Unter Aggregation von Daten wird die Zusammenfassung detaillierter Daten zu größeren Einheiten verstanden. Das ist eine der häufigsten Verarbeitungsschritte, die aus primären Daten (Rohdaten) sekundäre Daten (abgeleitete Daten) erstellt.[373]

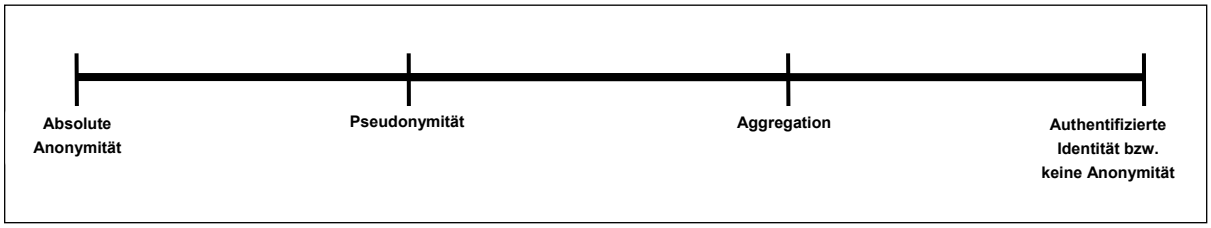

Abbildung 16: Grade der Anonymität[374]

Danach gibt es in einer Transaktion grundsätzlich drei Anonymitätsgrade, die anhand der Bekanntheit der Beteiligten wie folgt unterteilt werden können:

1. Absolute Identität - Keine Anonymität

2. Teilidentität - Pseudonymität - Partielle Anonymität

3. Absolute Anonymität

Im Folgenden werden die kurz dargestellten, verschiedenen Grade der Anonymität detailliert beschrieben.

---

370 Vgl. Spann/Zuber (2003), S. 13; Reiter/Rudin (1997) S. 3.

371 Vgl. Ebenda.

372 Vgl. Ebenda.

373 Vgl. http://www.uni-protokolle.de/Lexikon/Aggregiert.html, Stand: 25.10.2009.

374 In Anlehnung an Spann/Zuber (2003), S. 13.

4.4.1 Absolute Identität - Keine Anonymität

Die Identitäts- und Transaktionsdaten in Kommunikationsnetzwerken sind für alle, zumindest allen an einer Transaktion beteiligten Parteien zugänglich. Hier haben z. B. Dritte (Beobachter oder Angreifer) ein leichtes Spiel, Daten und Informationen über Personen, Instanzen sowie Gruppen zu sammeln und auswerten. Die Identität des Users ist allen an einer Transaktion beteiligten Parteien bekannt. Sowohl der Händler als auch die Banken bekommen die personenbezogenen Daten von Usern bei einer Transaktion. Die Händler und User müssen sich bei einer Transaktion gegenseitig identifizieren. So erhalten sie gegenseitig Daten und Informationen über den jeweiligen Partner. Banken und Kreditinstitute erhalten Kauf- und Userinformationen mittels elektronischer Zahlungssysteme.

Beispielsweise brauchen die Händler bei Mobile Payment, z.B. basierend auf Kreditkartensystemen, personenbezogenen Daten und Informationen von ihren Usern wie Name, Kontonummer, Wohnadresse etc. Manche User würden ihre personenbezogenen Daten und Informationen an den Händler oder anderen an der Transaktion beteiligten Parteien nicht preisgeben oder zögern diese einfach an den Händler auszuliefern. Auf der anderen Seite glauben manche Händler sogar, da die Mobile Payment mit Kreditkarten keine Anonymität für den User bietet, dass sie ihre Umsätze steigern könnten, wenn der User seine personenbezogenen Daten und Informationen nicht preiszugeben bräuchte.[375]

4.4.2 Teilidentität - Pseudonymität - Partielle Anonymität

Die User geben bei einer Registrierung beispielsweise um ein Gratisangebot zu erhalten oder einen Gratisservice zu nutzen, ihre personenbezogene Daten preis. Die User hinterlassen auf diese Weise viele Spuren. Aus diesen hinterlassenen Spuren werden die Teilidentitäten erstellt. Die Verkettung dieser Teilidentitäten stellt in digitaler bzw. virtueller Welt kein Problem dar.[376]

Bei der Teilidentität handelt es sich darum, dass eine Person in einer Kommunikation oder Transaktion nur Teile ihrer Identität dem Kommunikations- und Transaktionspartner mitteilt. Der Kommunikations- und Transaktionspartner kennt die wahre

---

[375] Vgl. Garfinkel/Spafford (2002), S. 620.

[376] Vgl. Ruedin (2009), S. 14ff.; Brown (2006).

Identität der Person nicht, sondern nur die digitale bzw. virtuelle Identität der Person, beispielsweise deren Pseudonyme.

Bei der Pseudonymität handelt es sich um die Veränderung des tatsächlichen Identifizierungskennzeichens oder der Erkennungsmarke durch ein Pseudonym. Ein Pseudonym ist ein beliebig gewähltes Kennzeichen, das einen Datensatz einer eindeutigen Person zuordnet, ohne deren Identität preiszugeben. Die eigentlichen Identitätsinformationen werden nicht bekanntgegeben oder übertragen. Pseudonyme können jedoch teilweise Informationen tatsächlicher Identitäten enthalten. Üblicherweise werden Pseudonyme in Verbindung mit den persönlichen Eigenschaften eingesetzt bzw. benutzt. Das Ziel der Pseudonymität ist nur bei Bedarf und unter Einhaltung der vorher definierten Rahmenbedingungen den Personenbezug herstellen zu können. Die Pseudonymität erlaubt also im Unterschied zur (absoluten) Anonymität eine Rückidentifizierung und bietet eine partielle Anonymität. Eine Rückidentifizierung kann in der Regel nur dem Betroffenen vorbehalten bleiben. Die Möglichkeit der Pseudonymität bzw. Pseudonymisierung kann unter Umständen dort verwendet werden, wo eine absolute Anonymität nicht möglich ist. Dies kommt dann in Frage, wenn nur eine Teilanonymität erwünscht ist oder der Aufwand für die Herstellung einer absoluten Anonymität groß ist.

Die Pseudonymisierung benutzt einen Schlüssel, mit dessen Hilfe die Möglichkeit der Zuordnung der Daten zu einer Person ausgeschlossen oder erschwert wird. Bei der Pseudonymisierung werden personenbezogene Daten und Identitätsmerkmale getrennt, bestehen jedoch immer noch die Möglichkeit der Zusammenführung der Person und Daten. Die Möglichkeit der Zusammenführung der Daten und Personen nimmt mit der Datenmenge, -qualität und -verfügbarkeit zu, da die Personen auch ohne den Schlüssel identifizierbar sind. Damit die Identifikation einer Person erschwert wird, soll ein Pseudonym verwendet werden, so dass die Person und personenbezogene Daten nicht direkt zuzuordnen sind. Wenn jedoch eine Person ganz anonym bleiben möchte, sollte sie die Möglichkeit der Anonymisierung nutzen. Mit der Anonymisierung ist unter anderem die Veränderung, Geheimhaltung oder auch Verfälschung persönlicher Informationen gemeint, um eine Identifizierung zu erschweren.

Es gibt im Verfahren der Pseudonymisierung drei Pseudonyme, die eine partielle Anonymität und gleichzeitig, je nach dem, eine Rückidentifizierung einer Person erlauben:[377]

- Usererstellte Pseudonyme
- Referenz-Pseudonyme
- Einweg-Pseudonyme

4.4.2.1 Usererstellte Pseudonyme

Usererstellte Pseudonyme sind von User selbst generiert und werden nicht mit den Daten und Informationen zusammen gespeichert und verwendet, die zur Identität der Person führen. Der User erstellt ein selbst gewähltes Pseudonym und benutzt das innerhalb eines Systems statt seinen wahren Namen zu verwenden. Eine Rückidentifizierung kann normalerweise nicht von den Service Providern durchgeführt werden und erfolgt nur durch die Person selbst. Die usererstellten Pseudonyme werden beispielsweise in wissenschaftlichen Studien verwendet, bei denen aggregierte Daten und Informationen über bestimmte Personengruppen gewonnen werden und einzelne Personen ihre persönlichen Einzelergebnisse teilanonym abrufen können.[378]

4.4.2.2 Referenz-Pseudonyme

Referenz-Pseudonyme werden von vertrauenswürdigen Dritten (TTP) oder Vertrauensstellen (Trust Centers) vergeben und für die Rückidentifizierung der Personen eingesetzt. Dazu werden Referenzlisten erstellt. Eine Rückidentifizierung kann nur über diese Referenzlisten erfolgen. Die Referenz-Pseudonyme können in den Systemen verwendet werden, in denen eine Rückidentifizierung beispielsweise bei Störfällen erforderlich ist. Um eine unbefugte Aufdeckung der Referenzpseudonyme zu verhindern und die Sicherheit der Referenzpseudonyme zu garantieren, sollten die Referenzlisten von den pseudonymisierten Daten räumlich und organisatorisch getrennt und bei mehreren TTPs gespeichert werden. Diese Referenzlisten oder -tabellen müssen streng geheim gehalten werden. Referenzpseudonyme werden in den Systemen verwendet, bei denen eine Rückidentifizierung der Person in be-

[377] Vgl. Ernestus et. al (1997), S. 6ff.
[378] Vgl. Ernestus et. al (1997), S. 6ff.

stimmten Ausnahmefällen z.B. bei fehlerhaften Zahlungstransaktionen erforderlich ist.[379]

4.4.2.3 Einweg-Pseudonyme

Einweg-Pseudonyme sind die Pseudonyme, die mittels Einweg-Funktion aus den personenbezogenen Daten meistens im asymmetrischen Verschlüsselungsverfahren erzeugt werden. Die Einweg-Funktion schließt mit hoher Wahrscheinlichkeit aus, dass die Identitätsdaten zweier Personen ein gemeinsames Pseudonym abgebildet werden. Die Identitätsdaten und das Pseudonym werden nicht durch eine Liste oder Tabelle wie bei Referenzpseudonymen in Verbindung gebracht, sondern durch eine explizit formulierte (parametrisierbare) Vorschrift hergestellt. Die Sicherheit der Einweg-Pseudonyme sollte nicht durch die Geheimhaltung dieser Vorschrift, sondern durch die Geheimhaltung der Parameter hergestellt sein.[380]

Bei den Einweg-Pseudonymen müssen die Identitätsdaten der Person in den Systemen nicht gespeichert werden, während dies bei den Referenz-Pseudonymen der Fall ist. Außerdem müssen die Instanzen, die die Pseudonyme verwalten und die geheimen Parameter kennen, von denjenigen Instanzen, die die pseudonymisierten Identitätsdaten verwenden, getrennt werden. Einweg-Pseudonyme werden für die Längsschnittuntersuchungen verwendet, bei denen nachträglich erhobene personenbezogenen Daten mit den Bestandsdaten zusammengeführt werden, ohne dass ein Personenbezug für die statistische Analyse der Daten erforderlich ist. Außerdem können die Einweg-Pseudonyme für die Auskunftssysteme verwendet, bei denen die Zugehörigkeit einer Person zu einer bestimmten Gruppe ermittelt wird, ohne dass die personenbezogene Identitätsdaten gespeichert werden müssen.[381]

4.4.3 Absolute Anonymität

Die absolute Anonymität liegt am anderen Ende des zuvor dargestellten Spannungsfeldes in der Abbildung 16, S. 101 und bedeutet genau das Gegenteil der absoluten Identität. Die Identitäts- und Transaktionsdaten in Kommunikationsnetzwerken sind nicht bekannt und nicht wie bei einer absoluten Identität zu den an einer Transaktion beteiligten Parteien zugänglich. Es besteht kaum eine Möglichkeit, Daten und

[379] Vgl. Ebenda; Pommerening (2007).

[380] Vgl. Ernestus et. al (1997), S. 7.

[381] Vgl. Ebenda.

Informationen über Personen, Instanzen sowie Gruppen zu sammeln und auswerten. Ein Beobachter bzw. Angreifer kann nicht einfach identifizieren, wer sich mit wem kommuniziert. Bei absoluter Anonymität kennen weder Kreditinstitute noch Händler die Identität von Usern. Der User hat die Möglichkeit seine Identität bei einer Rechtsfrage preiszugeben. Die Transaktionsdaten in Kommunikationsnetzwerken sind *nicht* für alle zugänglich. Nur diejenigen, die an einer Transaktion beteiligen, können diese zusammen offen legen.

4.5 Anonymität in stationären und mobilen Kommunikationsnetzwerken

4.5.1 Anonymität im Internet

Viele User surfen gegenwärtig im Internet nicht anonym, da viele User sich der Situation weder bewusst, noch in der Lage sind, dies zu kontrollieren. Dabei lässt sich jeder User im Internet sehr leicht identifizieren. Bei jeder Verbindung zum Internet werden den Usern die IP-Adressen von den Internetprovidern zugewiesen. Jeder Rechner bekommt eine eindeutige IP- und MAC-Adresse im Internet. Diese Adressen werden im Kommunikationsnetz bzw. Internet an andere Rechner bzw. Server gesendet. Die Internetprovider speichern die besuchten Webseiten und Userdaten mit Datum, Uhrzeit, Telefonnummer und zugewiesener IP-Adresse. Dabei werden die Cookies der Webserver auf lokalen Rechnern der User gespeichert, die wiederum die Userdaten ausspionieren. Durch die Kombination von IP-Adressen und Cookies können z. B. Userprofile erstellt werden. Ein Beobachter kann die Internetverbindungen, besuchte Seiten und Webadressen zurückverfolgen.[382] Ständige Abfragen persönlicher Daten und Registrierungen machen eine anonyme Internetnutzung schwierig. Die Userdaten werden gesammelt und gegen Geld gehandelt, beispielsweise Handel von Email-Adressen.[383] Mit den gesammelten Userdaten werden die Userprofile z. B. von Online-Marketingagenturen erstellt. Einige Portale wie z. B. MySpace oder Facebook besitzen bereits die Userprofile mit Namen, Adressen, Bildung und Hobbys etc. Die Userprofile werden mit den Surfprofilen kombiniert. Die Internetuser werden zu gläsernen Individuen. Auf diese Weise kann das Surf- und Kaufverhalten von Internetusern manipuliert und gesteuert werden.[384]

---

382 Vgl. Brown (2006).

383 Vgl. o. V. (2002).

384 Vgl. o. V. (2009a).

Anonyme Aktivität im Internet ist nur unter bestimmten Bedingungen realisierbar. In letzter Zeit wurden einige Methoden und Techniken für das anonyme Surfen, Shoppen, Kommunizieren sowie für die anonymen Transaktionen entwickelt und angewendet.[385] Die Grundidee dieser Methoden ist die Anonymisierung einer Kommunikation oder des Surfens innerhalb einer Gruppe von Internetusern, in dem die Rechner von Usern nicht direkt, sondern über Umwege zum Webserver verbunden werden. Jede Methode der Anonymisierung bestimmt damit den Anonymitätsgrad der User und gleichzeitig die Möglichkeiten eines Beobachters, User zu bewachen. Im Grunde könnten die Internetprovider Anonymisierungsdienste anbieten. Jedoch fehlen bisher ein breites Bewusstsein unter den Surfern bzw. Nachfrage nach Anonymisierungsdiensten. Es wird aber erwartet, dass sich diese Lage in den kommenden Jahren ändert.[386] Um eine breite Nachfrage nach Anonymisierungsdienste zu kreieren, können hier neue Business-Modelle auf der Grundlage vom Anonymitätsbedarfs und -wunschs entstehen.[387]

4.5.2 Anonymität im mobilen Netzwerken

Mit der zunehmenden Nutzung von mobilen Kommunikationsgeräten steigen auch Anforderungen an Sicherheit, Datenschutz und Anonymität. Das Thema Anonymität von Usern in mobilen Netzwerken ist bisher nur oberflächlich behandelt. Die aktuellen Techniken in mobilen Netzwerken berücksichtigen die Bedürfnisse nach Anonymität und Privatsphäre von mobilen Usern kaum. Heute ist noch kein anonymes Surfen mit mobilen Engeräten möglich. Die Mobilfunknetzbetreiber bekommen alle möglichen Informationen bezüglich der Identität und des Aufenthaltsorts von mobilen Usern und könnten ohne weiteres Daten über die mobilen User sammeln. Daher haben sie einen automatischen Zugriff auf die Userdaten und -informationen und könnten diese Userdaten und -informationen für verschiedene Zwecke benutzen. Viele existierende Lösungen zur Anonymität in mobilen und drahtlosen Netzwerken lassen sich in eine Gruppe von Entwürfen einordnen. Der Schutz der Privatsphäre wird auch in drahtlosen und mobilen Netzwerken angefordert.[388]

---

385 Vgl. mit den Erläuterrungen im Abschnitt 5.2.4 Anonymitätskonzepte, S. 124ff.

386 Vgl. o. V. (2007a).

387 Vgl. Kretschmann (2007).

388 Vgl. Hong/Kong/Gerla (2006), S. 283.

4.5.3 Anonymität im Mobile Commerce

Eine wichtige Anforderung an Mobile Commerce ist die Anonymität und Schutz eigener Identität. Beispielsweise möchte man Geschäftsbeziehungen anderen Menschen nicht mitteilen. Man hat einfach mehrere Beziehungen mit seiner Umgebung wie Geschäftspartner, Firmen, öffentliche Verwaltungen etc. gleichzeitig, ist auch die Anforderung an Anonymität gestiegen. Insbesondere spielt die Kommunikationsanonymität von mobilen Usern in Mobile Business Anwendungen eine große Rolle.

Tatli et al. beschreiben in ihrem Beitrag, dass die User bzw. Kommunikationspartner und Applikationen andere Sensibilitäten im Mobile Business als im Internet haben. Sie reden von der dynamischen Anonymität und schlagen einen Lösungsansatz für Mobile Business vor.[389] Danach werden mobile Endgeräte für Geschäftstransaktionen eingesetzt. Service Provider bieten User kostenlose oder zahlungspflichtige Inhalte an. User erhalten diese Dienstleistungen, in dem sie ihre mobilen Endgeräte einsetzen. Die Vermittler registrieren diese Dienstleistungen und liefern diese an die User. Hier nimmt der Vermittler die Rolle einer TTP. Die Risiken im Mobile Business weisen auf die Anonymität und den Schutz personenbezogener Daten. Um eine absolute Anonymität zu ermöglichen, müssen sowohl Content-Anonymität als Kommunikationsanonymität erfüllt sein. Pseudonyme bieten Content-Anonymität, können aber die Kommunikationsanonymität nicht erfüllen, da ein Beobachter zwar den Inhalt der Kommunikation nicht erfahren, jedoch eine Beziehung zwischen den kommenden und gehenden Nachrichten herstellen kann. Somit ist er in der Lage, sich nachzuvollziehen, wer mit wem kommuniziert. Dieses Risiko kann durch Gewährleistung der Unverkettbarkeit (Unlinkability) abgewendet werden.[390]

4.6 Bewertung der Anonymität

Die Themen Anonymität und Pseudonymität werden im Zusammenhang mit dem Schutz der Internet- bzw. webbasierten Kommunikation und Transaktionen kontrovers diskutiert. Während dieser Diskussion auf öffentlicher und wissenschaftlicher Plattform werden Gründe, Vorteile und Nachteile ausgeführt. Palme fasst in seinem Beitrag basiert auf den Thesen von Berglund die Pro und Contra Anonymität

[389] Vgl. Tatli/Stegemann/Lucks (2006), S. 1ff.
[390] Vgl. Ebenda, S. 2ff.

und Pseudonymität zusammen.[391] Palme und Berglund erklären, dass Anonymität und Pseudonymität für gute und schlechte Zwecke verwendet werden können. So kann Anonymität beispielsweise für eine Person, Instanz, Institution, Organisation oder Gruppe von Personen wünschenswert bzw. für eine andere Person, Instanz oder Gruppe von Personen nicht wünschenswert sein. Deshalb soll im Folgenden gezeigt werden, welche Argumente für und gegen die Anonymität bzw. Pseudonymität erhoben werden, um deren Natur und Notwendigkeit für die Kommunikation und Transaktionen zu verstehen.

4.6.1 Pro Anonymität

Für die Anonymität und Pseudonymität der Personen und deren Aktivitäten in stationären und mobilen Kommunikationsnetzen werden folgende Argumente erhoben:

- Personen, die abhängig von einer Organisation sind oder Angst vor Rache haben, können ernsthaften Missbrauch enthüllen, der offenbart werden sollte. Anonyme Tipps können als eine Informationsquelle von Zeitungen so wie auch Polizei und Sicherheitsbehörden verwendet werden, die aufgrund anonymer Anzeigen Kriminellen auf der Spur sind. Nicht jeder wird solche anonyme Kommunikation für gut halten. Beispielsweise wurden Foren für die Mitarbeiter außerhalb der Firma errichtet, um ihre Meinungen über ihre eigenen Firmen anonym abzugeben.[392] Bei polizeilichen Untersuchungen wird die Anonymität zur komplexen Frage, da die Sicherheitsbehörden die Identität des anonymen Informanten erfahren möchten, um weitere Informationen zu erhalten oder sicherzugehen, dass der anonyme Informant zuverlässige Infos liefert oder sogar als Zeuge auftrifft.[393]

- Personen, die in einem autoritären und totalitären Regimes leben und wegen ihrer politischen Ansichten und Meinungen unterdrückt bzw. verfolgt werden, können Anonymität und Pseudonymität nutzen, um eine Verfolgung durch die vorgenannten Regimes zu vermeiden. Beispielweise können diese Menschen im Internet anonyme

---

391 Vgl. Palme/Berglund (2004).

392 Vgl. Im Portal von Kununu können sich aktuelle und ausgeschiedene Mitarbeiter ihre Meinungen sowohl für die Bewerber als auch Firmen anonym äußern. Kununu ist eine webbasierte Plattform, die es Arbeitnehmern in Österreich, Deutschland und der Schweiz ermöglicht, Arbeitsverhältnisse in Unternehmen anonym zu bewerten. URL: http://www.kununu.com/, Stand: 29.10.2009.

393 Vgl. Palme/Berglund (2004).

Server in anderen Ländern verwenden, um ihre Identität vor Verfolger oder Beobachter schützen.[394]

- Personen können mit Hilfe der Anonymität und/oder Pseudonymität ganz offen mit anderen Personen über ihre persönliche Probleme oder Angelegenheiten diskutieren, die normalerweise für sie peinlich wären wie z. B. sexuelle Probleme zu erzählen.[395]

- Personen können mehr objektive Bewertung Ihrer Nachrichten von anderen Personen erhalten, ohne dass sie ihre richtigen Namen nennen müssen.[396]

- Personen treten in anonymen Diskussionen gleich auf, ohne dass die Faktoren wie Status, Geschlecht, Herkunft etc. keinen bzw. minimalen Einfluss darauf haben, was sie sagen und erzählen.[397]

- Pseudonymität bietet Menschen auch die Möglichkeit, mit verschiedenen Rollenspielen zu experimentieren, um andere besser verstehen zu können. Beispielsweise kann sich ein Mann unter einem Pseudonym als eine Frau ausgeben, um die Gefühle von anderem Geschlecht besser verstehen zu können.[398]

- Pseudonymität kann als ein Werkzeug für schüchternen Menschen eingesetzt werden, um Kontakte zu anderen Menschen herzustellen.[399]

Der Schutz der Privatsphäre der Personen in den stationären und mobilen Kommunikationsnetzen muss genau so wie im realen Leben gewährleistet und sowohl organisatorisch bzw. technisch als auch rechtlich adäquat gestaltet werden. Mit der datenschutzkonformen Gestaltung der Kommunikationsnetze müssen die Personen und deren Aktionen vor einer teilweisen und totalen Überwachung geschützt werden. Außerdem dürfen die Personen selbst entscheiden können, ob und wie sie ihre Identität preisgeben möchten. Der Wunsch zur Anonymität der Personen bzw. deren Aktionen ist nicht verwerflich, sondern das ist ein Grundrecht der Personen.

---

394 Vgl. Palme/Berglund (2004).
395 Vgl. Ebenda.
396 Vgl. Ebenda.
397 Vgl. Ebenda.
398 Vgl. Ebenda.
399 Vgl. Ebenda.

4.6.2 Contra Anonymität

Gegen Anonymität und Pseudonymität der Personen und deren Aktivitäten in stationären und mobilen Kommunikationsnetzen werden folgende Argumente erhoben:

- Anonymität kann unter Umständen Schutz für kriminelle Personen bieten und von kriminellen Personen oder Gruppen missbraucht werden, um Verbrechen zu begehen. Beispielsweise können unter Verwendung der Anonymität z. B. vorsätzliche Schäden wie die Verteilung von Computerviren etc. ausgeübt werden.[400]

- Anonymität kann missbraucht werden, um Kontakte zu verknüpfen, mit denen man illegale Aktivitäten durchführen könnte. Beispielsweise kann ein Betrüger Leute suchen, die er abzocken kann.[401]

- Auch wenn die Aktivitäten nicht illegal sind, könnte die Anonymität für aggressive oder störende Kommunikation missbraucht werden. Beispielsweise kann die Anonymität missbraucht werden, um sich über andere üble Dinge zu äußern.[402]

Zusammenfassend kann festgehalten werden, dass jedes Argument aus eigenem Punkt heraus betrachtet werden sollte. Bei der Realisierung der datenschutzkonformen Kommunikationsnetze sollte zwischen den Argumenten abgewogen und situationsbezogen entschieden werden, so dass es zwischen den Interessen der Personen und anderen Beteiligten eine Balance gibt.

4.7 Bedeutung der Anonymität in Mobile Payment Systemen

Auf die Frage, warum die Anonymität in einer modernen Gesellschaft wichtig ist, werden die Antworten aus soziologischer und ökonomischer Sicht gegeben, die auch für die User-Anonymität von großer Bedeutung sind.

Aus soziologischer Sicht wird die Anonymität als „konstitutiv“ bezeichnet, weil es in modernen Gesellschaften ein großer Bedarf nach Nichtzurechenbarkeit von Kommunikationen und Handlungen auf Personen besteht. Die Nichtzurechenbarkeit

---

400 Vgl. Palme/Berglund (2004).

401 Vgl. Ebenda.

402 Vgl. Ebenda.

ermöglicht auf individueller Ebene eine gewisse Unabhängigkeit und Freiheit, und auf der sozialen Ebene eine Wahlmöglichkeit zwischen den Alternativen. [403]

Aus ökonomischer Sicht spielt die Anonymität auch eine wichtige Rolle. Beim Geldtausch wird von einer „sozialen Beziehung mit einem Unbekannten“ gesprochen, dessen Identität gleichgültig ist und auch so bleibt. Beim Erwerb eines Gutes wird Geld getauscht und braucht es dabei nicht immer auch persönliche Daten zu tauschen. Das heißt, man gibt das Geld hin und nimmt das Gewünschte entgegen, ohne dass mit diesem Tausch auch zwangsläufig die persönlichen Daten gewechselt werden müssen. Man geht in der Form des Geldtausches eine soziale Beziehung auch mit demjenigen ein, den man nicht kennt, der einem gleichgültig ist und der dies normalerweise auch weiterhin bleiben kann.[404]

Das Interesse und die Bedeutung der Anonymität kann auch für die innovativen mobilen Zahlungssysteme mit den Argumenten der beiden Disziplinen erklärt werden. Daraus kann abgeleitet werden, dass es beim Erweb eines Gutes oder Services, die mit den modernen mobilen Zahlungssystemen bezahlt werden, nicht immer auch persönliche Daten ausgetauscht werden müssen. Ein sehr wichtiger Aspekt des konventionellen (Bar-)Geldes ist seine Anonymität. Beim Bargeld kann zwischen den Zahlungen und den gekauften Produkten keine Beziehung hergestellt werden, so dass die User dadurch anonym kaufen können. Das Bargeld (Physisches Geld) ermöglicht es dem User, bezüglich der Nutzung des Geldes anonym zu bleiben, da das Bargeld keine Merkmale besitzt, die es unmittelbar dem User zuordnen.[405] Der User würde sich daher diese Eigenschaft des Bargeldes, nämlich die anonyme Nutzung des Geldes auch in Mobile Payment Systemen wünschen.

Das Vertrauen von Kunden in Mobile Payment kann durch die verschiedenen Formen der Anonymität erhöht werden. So sollen die Zahlungstransaktionen durch Unbeteiligte unbeobachtbar und unverkettbar sein. Eine hundertprozentige Anonymität in Mobile Payments gibt es derzeit nicht. Allerdings sollte darauf geachtet werden, dass die Identifizierung eines Users so schwer wie möglich gestaltet werden muss, damit sich der Aufwand eines Versuchs zu seiner Identifizierung nicht lohnt. Allerdings sollten bei der Gestaltung der Anonymität auch die Interessen anderer Marktteilnehmer berücksichtigt werden.

---

[403] Vgl. ULD (2002), S. 39ff.; Rost (2003), S. 158.

[404] Vgl. Ebenda.

[405] Vgl. Hansen/Meissner (2007), S. 107.

5 Rahmenbedingungen der User-Anonymität

Für die Gestaltung der User-Anonymität in stationären und mobilen Kommunikationsnetzwerken sollen Rahmenbedingungen geschaffen werden. Hierfür sollen die vorhandenen Möglichkeiten analysiert und gezeigt werden. Gegebenenfalls sollen neue Möglichkeiten für die Gestaltung der User-Anonymität untersucht werden. Zu diesem Zweck wird in diesem Kapitel eine Übersicht über die Gestaltungsmöglichkeiten der User-Anonymität in stationären und mobilen Kommunikationsnetzwerken, also im Internet und Mobile Commerce gegeben. Die Rahmenbedingungen der User-Anonymität umfassen die folgenden Gestaltungsmöglichkeiten und Realisierungsschritte und -maßnahmen:

- Organisatorische Rahmenbedingungen der User-Anonymität
- Technische Rahmenbedingungen der User-Anonymität
- Rechtliche Rahmenbedingungen der User-Anonymität

Für eine erfolgreiche Realisierung der User-Anonymität sollen alle Rahmenbedingungen und Maßnahmen parallel berücksichtigt, getroffen und umgesetzt werden. Dies kann erst durch das Zusammenspiel und einzelnen Aktivitäten der Interessensgruppen erfolgen. Im Folgenden sollen die drei Rahmenbedingungen der User-Anonymität detailliert analysiert werden.

5.1 Organisatorische Rahmenbedingungen der User-Anonymität

Für die Gestaltung der User-Anonymität sollen die organisatorischen Rahmenbedingungen gegeben sein. Welche organisatorischen Rahmenbedingungen dafür erforderlich sind, hängt von der organisatorischen Gestaltung der Geschäftsprozesse sowie der Organisation der darunter fallenden User- und Geschäftsdaten und Informationen ab. Deshalb wird im Folgenden erklärt, was sich hinter Daten und Informationen verbirgt und wie sie sich in den Geschäftsprozessen widerspiegeln. Hierfür werden zunächst Daten und Informationen definiert und die Organisation der Daten und Informationen erklärt. Danach wird die Behandlung der Daten und Informationen in den Geschäftsprozessen erläutert.

5.1.1 User- und Geschäftsdaten und Informationen

5.1.1.1 Definition und Organisation der Daten

Stahlknecht und Hasenkamp definieren den Begriff Daten wie folgt: „*Daten sind nach ISO/IEC 2381-1 eine Darstellungsform von Informationen, die für Kommunikation, Interpretation und Verarbeitung geeignet ist.*“ Außerdem definieren beide Autoren den Begriff Datenorganisation wie folgt: „*Unter dem Begriff Datenorganisation werden alle Verfahren zusammengefasst, die dazu dienen, Daten bzw. Datenbestände zu strukturieren, d. h. hinsichtlich ihrer Zusammenhänge zu analysieren und zu ordnen (logische Datenorganisation) und auf peripheren Speichern, insbesondere auf (magnetischen oder optischen) Platten zu speichern und für den Zugriff verfügbar zu halten (physische Datenorganisation oder Datenhaltung).*“[406]

Die logische Datenorganisation wird wie folgt definiert: „*Die logische Datenorganisation befasst sich mit Datenobjekten, die durch ihre Eigenschaften (Attribute oder Merkmale) beschrieben werden.*“[407] Bespiele für solche Datenobjekte können Personen, Gegenstände und abstrakte Begriffe sein:[408]

- Personen: Kunden, Lieferanten, Mitarbeiter, Kontoinhaber etc.
- Gegenstände: Handelswaren, Rohstoffe, Maschinen, Gebäude etc.
- Abstrakte Begriffe: Konten, Buchungen, Bestellungen, Rechnungen, Verträge etc.

Neben der Definition und Organisation der Daten werden auch die Einsatzformen und Verfahren der Daten erklärt. Stahlknecht und Hasenkamp erklären die Einsatzformen der Daten vom Verwendungszweck her. Sie unterscheiden bei den klassischen betriebswirtschaftlichen operativen Systemen zwischen Stamm-, Bestands- sowie Bewegungs- und Änderungsdaten.[409]

In der Telekommunikation fallen viele verschiedene Daten an. In der Literatur werden zahlreiche Kategorisierung dieser Daten genannt, deren Definitionen jedoch nicht

---

[406] Vgl. Stahlknecht/Hasenkamp (2005), S. 131.

[407] Vgl. Ebenda, S. 134.

[408] Vgl. Ebenda, S. 134 und 135; Hansen/Neumann (2009), S. 9 ff. In beiden Werken geben Autoren ausführliche Informationen und Beispiele für die logische Datenorganisation.

[409] Vgl. Stahlknecht/Hasenkamp (2005), S. 137; Hansen/Neumann (2009), S. 9ff.

klar sind und sich oft überschneiden.[410] Zur Vereinfachung werden drei Datenkategorien für die Datenerhebung und Datenverwendung, wie in der Abbildung 17 dargestellt, verwendet.[411] Danach werden zwischen Bestands-, Verkehrs- und Standortdaten unterschieden. Unter Bestandsdaten werden Stammdaten, also personenbezogenen Daten eines Users verstanden. Als Verkehrsdaten werden die Verbindungsdaten verstanden, die bei der Erbringung eines Telekommunikationsdienstes auftauchen. Diese können auch als Transaktionsdaten bezeichnet werden. Standortdaten sind die Daten, die den Standort des Mobilfunkgerätes eines Users angeben. Die drei Datenkategorien werden in den folgenden Abschnitten näher behandelt.

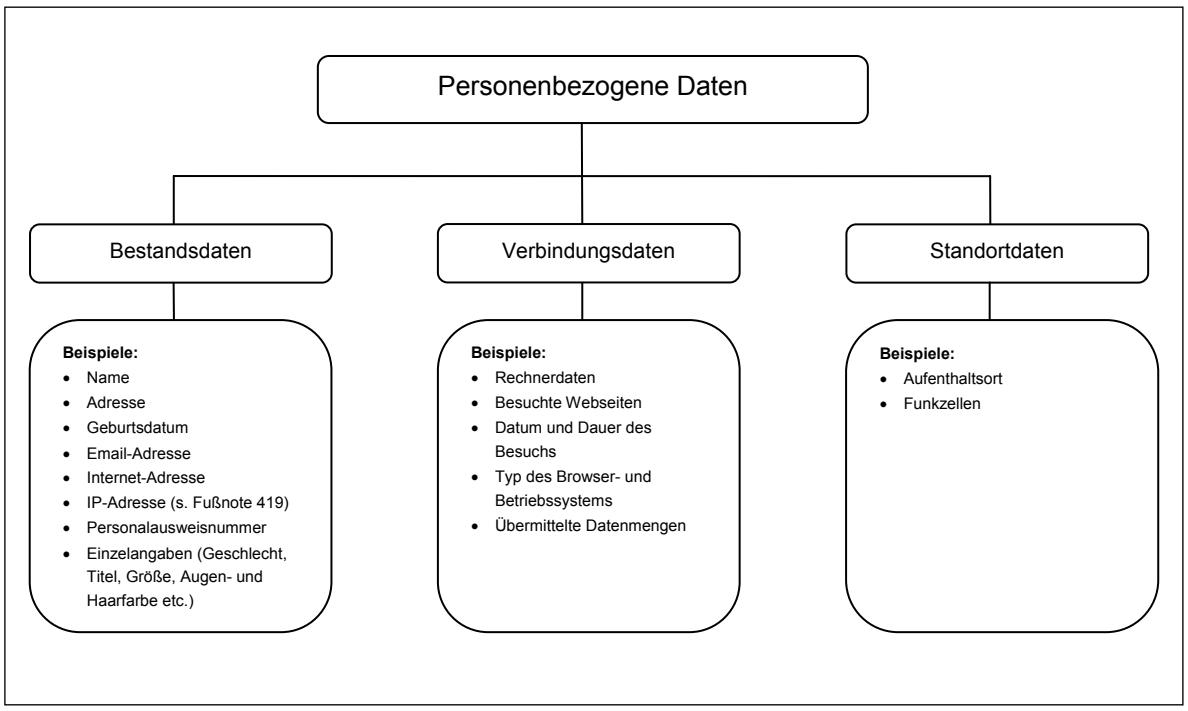

Abbildung 17: Kategorien personenbezogener Daten

Im nächsten Abschnitt erfolgt die begriffliche Unterscheidung zwischen Information, Daten und Metadaten, um eine Klarheit dieser Begriffe zu schaffen.

410 Vgl. Fischer/Keil-Slawik/Richter (2001), S. 68.

411 Vgl. Kühling/Sivridis/Seidel (2008), S. 273.

5.1.1.2 Begriffliche Unterscheidung zwischen Daten, Information und Metadaten

Unter dem Begriff Daten versteht man die Information in einer maschinell verarbeitbaren Form. Der Schwerpunkt liegt dabei auf der Spezifikation der Syntax (Form).[412] Daten sind somit eine Ansammlung von definierten Werten oder formalisierten Inhalten wie Wörter, Zahlen, Bilder, beispielsweise auf einem digitalen Speicher in Form von Einsen und Nullen, auf einem Papier als Ziffer und Zeichen. Daten sind potentiell nutzbare Informationen.

Unter dem Begriff „Information" versteht man die Angaben über die Sachverhalte und Vorgänge. Die Information beinhaltet Syntax (Form) und Semantik (Inhalt).[413] Die Information entsteht erst durch die Deutung der Daten und Herstellung eines Sinnzusammenhangs. Außerdem wird unter Information die Übertragung von Daten zwischen Sender und Empfänger verstanden.

Metadaten sind Informationen über andere Daten und enthalten Angaben über die Eigenschaften eines Objektes. Mit anderen Worten können unter Metadaten (Daten über Daten) strukturierte Daten verstanden werden, mit deren Hilfe eine Informationsressource beschrieben und dadurch besser auffindbar gemacht wird.*"*[414] Die W3C-Konsortium definiert Metadaten wie folgt: *"Metadaten sind maschinenlesbare Informationen über elektronische Ressourcen oder andere Dinge. Metadaten liefern also Grundinformationen über ein Dokument, wie z. B. Angaben über Autor, Titel oder Zeitpunkt der Veröffentlichung."* [415]

Zusammenfassend kann festgehalten werden, dass Daten bzw. Metadaten durch die Interpretation zu Informationen umgewandelt werden. Diese Informationen können wiederum miteinander verkettet werden, um zu einem aktiv vorhandenen, abrufbaren und übertragbaren Wissen zu gelangen.

---

412 Vgl. Hansen/Neumann (2009), S. 6.

413 Vgl. Ebenda.

414 Ausführliche Informationen über die Metadaten unter http://www2.sub.uni-goettingen.de/intro meta.html, Stand: 09.08.2009.

415 Vgl. http://www2.sub.uni-goettingen.de/intrometa.html und http://www.w3.org/Metadata/, Stand: 09.08.2009.

5.1.2 Bestandsdaten und personenbezogene Daten

Bestandsdaten sind personenbezogene Daten[416], die dem Datenschutzgesetz unterliegen. Gemäß § 3 Nr. 3. TKG sind Bestandsdaten wie folgt definiert:

„*"Bestandsdaten"* sind *Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden.*“[417]

Danach werden unter Bestandsdaten solche personenbezogenen Daten über einen User verstanden, die meistens in einer Datenbank auf Dauer bei einem Service Provider gespeichert sind, die für Vertrags- und Abrechnungszwecke zwischen dem Service Provider und User benötigt werden.[418] Diese Daten sind insbesondere Personalien eines Users wie Name, Geburtsdatum, Beruf, etc. Unter personenbezogenen Daten werden Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder einer bestimmbaren natürlichen Person verstanden. Beispiele für die personenbezogenen Daten sind wie in der Abbildung 17, S. 115 dargestellt:

- Name
- Adresse
- Geburtsdatum
- Telefonnummer
- Email-Adresse
- Internet-Adresse
- IP-Adresse[419]
- Personalausweisnummer
- Einzelangaben wie Geschlecht, Titel, Größe, Augen- und Haarfarbe etc.

---

416 Vgl. Kühling/Sivridis/Seidel (2008), S. 100ff.

417 Vgl. TKG § 3 Begriffsbestimmungen, http://bundesrecht.juris.de/tkg_2004/__3.html, Stand: 11.08. 2009.

418 Vgl. Fischer/Keil-Slawik/Richter (2001), S. 69.

419 Ob statische oder dynamische IP-Adressen zu den Bestandsdaten als personenbezogenen Daten oder Verkehrsdaten (Verbindungsdaten) gehören, ist umstritten. Vgl. http://lawgical.jura.uni-sb.de/index.php?/entry/393-Achtung-IP-Adressen-sind-keine-Bestandsdaten!.html, Stand: 11.08. 2009.

5.1.3 Behandlung der Bestandsdaten und personenbezogener Daten

In der Regel werden personenbezogene Daten wie Name, Anschrift, Telefonnummer oder E-Mail-Adresse nicht gespeichert. Jedoch gibt es eine Ausnahme. Wenn der User diese Angaben freiwillig macht, z. B. im Rahmen einer Registrierung, einer Umfrage etc., werden auch diese Daten zusammengespeichert.[420] Bezüglich der Nutzung und Weitergabe personenbezogener Daten verwenden Unternehmen diese Daten unter anderem zur technischen Administration der Webseiten oder zur Abwicklung des mit Usern geschlossenen Vertrages bzw. zur Beantwortung der Anfrage von Usern.[421] Außerdem nutzen Unternehmen diese Daten für produktbezogene Umfragen oder Marketingzwecke, wenn User ihre Einwilligung erteilt oder keinen Widerspruch eingelegt haben.

Sowohl private Institutionen z. B. Auskunfteien als auch staatliche Stellen z. B. Geheimdienste, Polizei etc. interessieren sich für personenbezogene Daten. Daher wird im deutschen Datenschutzrecht zwischen dem privaten und öffentlichen Bereich unterschieden. Während es auf dem öffentlichen Bereich eine Reihe von Gesetzen, Rechtsvorschriften gibt, wie öffentliche Stellen mit Daten umgehen sollen, gibt es im privaten Bereich wenige Regelungen für den Datenschutz. Die öffentlichen Stellen müssen eine gesetzliche Erlaubnis für eine Verarbeitung personenbezogener Daten bringen. Im privaten Bereich ist das weniger konkret geregelt.[422]

In der Regel dürfen Unternehmen personenbezogene Daten weder weitergeben, noch verkaufen oder an Dritte übermitteln. Jedoch können Unternehmen dies tun, wenn es zur Vertragsabwicklung erforderlich ist oder User ihre Einwilligung erteilt haben. Beispielsweise kann es erforderlich sein, dass Unternehmen bei Bestellungen von Produkten die Anschrift und Bestelldaten an die Lieferanten weitergeben.[423]

Das Erheben von Bestandsdaten durch den Telekommunikationsdienstanbieter ist davon abhängig, welche dieser Bestandsdaten er für die Erbringung der Dienste benötigt. Abgesehen von § 111 TKG besteht keine Pflicht zur Erhebung bestimmter

---

420 Vgl. mit dem Abschnitt 5.3 Regulatorische Rahmenbedingungen der Anonymität, S. 140.

421 Vgl. Fischer/Keil-Slawik/Richter (2001), S. 69.

422 Vgl. Ausführliche Informationen finden sich unter http://www.datenschutz.de/recht/fundament/datenschutz/, Stand: 10.09.2009. Auf die Thematik der Vorratsdatenspeicherung wird im Abschnitt 5.3 Regulatorische Rahmenbedingungen der Anonymität, S. 140 sowie im Abschnitt 5.3.2.1 Vorratsdatenspeicherung und Überwachung der Netzwerke, S. 148 eingegangen.

423 Vgl. Ebenda.

Bestandsdaten des Users durch den Telekommunikationsdienstanbieter. Nach § 113 TKG haben Unternehmen und Personen über personenbezogene Daten, die sie für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses erhoben haben, im Einzelfall auf Verlangen an die zuständigen Stellen (zum Beispiel Polizei, Staatsanwaltschaft, Gerichte) unverzüglich Auskunft zu erteilen, soweit dies für die Verfolgung von Straftaten und Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes sowie des Zollkriminalamtes erforderlich ist.[424]

5.1.4 Verbindungsdaten und Transaktionsdaten

Verbindungsdaten werden im TKG als Verkehrsdaten bezeichnet. Die Legaldefinition der Verbindungsdaten ist in § 3 Nr. 30 bestimmt:[425]

„*"Verkehrsdaten"* sind *Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden.*“

Danach sind die Verbindungsdaten oder Verkehrsdaten die technischen Daten, die bei der Nutzung eines Telekommunikationsdienstes wie Telefonie und Internetnutzung beim jeweiligen Telekommunikationsdienstanbieter anfallen und von diesem erhoben, gespeichert, verarbeitet, übermittelt oder genutzt werden können. Als Verbindungsdaten oder Verkehrsdaten werden folgende Daten bezeichnet:[426]

- der genutzte Telekommunikationsdienst
- die Nummer oder die Kennung der beteiligten Anschlüsse (Anrufer und Angerufener)
- personenbezogene Berechtigungskennungen
- die Kartennummer (bei Verwendung von Kundenkarten)
- Standortdaten bei Mobiltelefonen

---

[424] Die Gesetze, Rechtsvorschriften und Regelungen für den Schutz personenbezogener Daten werden im Abschnitt 5.3 Regulatorische Rahmenbedingungen der Anonymität, S. 140ff. ausführlich erklärt.

[425] Vgl. TKG § 3 Begriffsbestimmungen, http://bundesrecht.juris.de/tkg_2004/__3.html, Stand: 11.08. 2009.

[426] Vgl. Koch (2005), S. 920ff.

- Beginn und Ende der jeweiligen Verbindung (Datum und Uhrzeit)
- die übermittelten Datenmengen

Unter Verbindungsdaten fallen auch Transaktionsdaten. Eine Transaktion wird als …*die Zusammenfassung logisch zusammengehörender Einzeloperationen (auch Aktionen genannt)*[427] … oder … eine logisch zusammengehörige Folge von Operationen[428] … definiert. Bei einer Transaktion werden verschiedene Daten ausgetauscht, die man als Transaktionsdaten bezeichnet. Als Transaktionsdaten werden beispielsweise für eine Kauf bzw. Verkauftransaktion folgende Daten in einer Datenbank erfasst:

- Transaktionsnummer
- Ware
- Kaufdatum
- Kaufzeitpunkt
- Kaufmenge
- Kaufbetrag
- Zahlungsart
- Mehrwertsteuer

5.1.5 Behandlung der Verbindungs- und Transaktionsdaten

Unternehmen geben auf ihren Webseiten in der Datenschutzklausel an, dass die Informationen, die nicht direkt mit den User der Webseiten in Verbindung gebracht werden können, wie z. B. Favoriten der Webseiten (Lesezeichen für die meistbesuchten Webseiten) oder Anzahl der User einer Webseite, keine personenbezogenen Daten sind. Daher speichern sie besuchte Webseiten für einen Zeitraum aus verschiedenen Gründen, wie sie selber angeben, unter anderem aus Systemsicherheitsgründen. Dabei werden folgende Daten und Informationen gespeichert:

- Verbindungsdaten des anfragenden Rechners
- besuchte Webseiten

---

[427] Vgl. Dadam (1996), S. 185.

[428] Vgl. http://www.enzyklopaedie-der-wirtschaftsinformatik.de/wi-enzyklopaedie/lexikon/daten-wissen/Datenmanagement/Datenbanksystem/Transaktion, Stand: 11.08.2009.

- Datum und Dauer des Besuches
- Erkennungsdaten des verwendeten Browser- und Betriebssystems sowie
- Webseite, von der aus User die Webseite besuchen

Die Verbindungsdaten betreffen nicht den Inhalt, jedoch die Umstände dieser Kommunikation. Durch die Verbindungsdaten kann festgestellt werden, wer mit wem wie lange kommuniziert und welche Art von Daten ausgetauscht hat.[429] Transaktionsdaten werden neben der Nutzung für die Abwicklung der Geschäfte auch zur Informationsgewinnung im Marketing und anderen Bereichen durch verschiedene Methoden wie Data Mining genutzt. Dies geschieht mit der Analyse der personalisierten oder anonymen Transaktionen in einer Datenbank. Dadurch bietet sich die Möglichkeit, einerseits Kaufmuster im Zeitablauf zu analysieren, andererseits die Transaktionen mit den soziodemografischen Daten in Beziehung zu bringen, um Käuferprofile zu erstellen und das Kaufverhalten zu analysieren. Damit erhalten die Anbieter von Produkten und Dienstleistungen Einblicke in Käuferprofile und Kaufverhalten und somit Marktmacht gegenüber dem Käufer. Jedoch können diese Anbieter solche Analysen auch für die Verbesserung der Kommunikation und zur Gestaltung der Angebots- und Sortimentgestaltung einsetzen. Mit den personalisierten Transaktionsdaten lassen sich wertvolle Informationen für die Identifizierung der Käufer(Segmente) gewinnen.[430]

5.1.6 Standortdaten und deren Behandlung

Standortdaten betreffen insbesondere die Verarbeitung der in Location Based Services anfallenden Daten.[431] Standortdaten werden im TKG als Verkehrsdaten bezeichnet. Die Legaldefinition der Standortdaten ist in § 3 Nr. 19 bestimmt:[432]

„*"Standortdaten" Daten, die in einem Telekommunikationsnetz erhoben oder verwendet werden und die den Standort des Endgeräts eines Endnutzers eines Telekommunikationsdienstes für die Öffentlichkeit angeben.*“

---

[429] Vgl. Fischer/Keil-Slawik/Richter (2001), S. 69.

[430] Vgl. Schröder/Rödl (2004), S. 519 ff.

[431] Vgl. mit den Erläuterungen im Abschnitt 2.1.2 Location Based Services, S. 14.

[432] Vgl. TKG § 3 Begriffsbestimmungen, http://bundesrecht.juris.de/tkg_2004/__3.html, Stand: 11.08. 2009 sowie mit den Erläuterungen im Abschnitt 5.1.4 Verbindungsdaten und Transaktionsdaten, S. 119.

Bei mobilen Usern können der Standort (geographische Lage) der User und der Ort der Kommunikation, also die jeweilige Funkzelle, in der sich der mobile User befindet bzw. befand, ermittelt werden.[433] Durch die Kombination der Standort- und Verbindungsdaten können Bewegungsprofile mobiler User erstellt werden.[434]

5.2 Technische Rahmenbedingungen der Anonymität

Für die technische Realisierung der Anonymität existieren verschiedene Technologien, technischen Verfahren und Konzepte, die eine weitgehende Anonymität gewährleisten und Schutz vor den Beobachtern bzw. Angreifern bieten. Die existierenden technischen Lösungen und Konzepte zur Anonymität können wie folgt dargestellt werden:

- anonyme Server Systeme
- anonyme Netzwerke
- anonyme Protokolle
- anonyme Transaktionen
- Anonymitätskonzepte

Im Folgenden sollen die einzelnen Technologien, Verfahren und Konzepte und deren Funktionsweise und Anonymitätsgrade detailliert gezeigt werden. Die Anonymitätskonzepte werden aufgrund der Relevanz detaillierter beschrieben.

5.2.1 Anonyme Server Systeme

Anonyme Server Systeme ermöglichen das Absenden von Email-Nachrichten an den Empfängern in anonymisierter oder pseudonymisierter Form, in dem sie E-Mail-Header, also die Daten, die auf die Identität des Senders hinweisen, entfernen, so dass der Empfänger nicht erfährt, wer die Email-Nachricht ursprünglich gesendet hat. Beispielsweise kann ein User in einem Forum oder jemandem anonyme Nachrichten

---

[433] Vgl. Kühling/Sivridis/Seidel (2008), S. 276.

[434] Vgl. dazu auch mit den Erläuterungen im Abschnitt 5.3.2.3 Herausgabe der Bestandsdaten, S. 150 sowie 5.3.2.4 Herausgabe der Verkehrsdaten, S. 151.

senden, ohne dass er seinen Namen und seine Email-Adresse preisgibt. Beispiel: Anonymous Remailer oder Pseudonymous Remailer[435]

Durch den Einsatz asymmetrischer Verschlüsselungsverfahren kann die Sicherheit der anonymen Server Systeme nochmals erhöht werden. Das Verfahren kann außerdem einfach zu einem Pseudonymous Remailer erweitert werden, wenn die User Antwort auf ihre Email-Nachrichten bekommen möchten, in dem jeder User ein Pseudonym nutzt. Das Verfahren ist jedoch nicht ganz anonym, da die Betreiber der anonymen Server die Identität von Usern enthüllen können. Die Betreiber müssen deshalb das Vertrauen der User gewinnen.[436]

5.2.2 Anonyme Netzwerke

Der Zweck anonymer Netzwerke ist die Herstellung und Sicherung der Client-Anonymität. Das heißt, ein Webserver kann durch anonyme Netzwerke seinen Client nicht erkennen. Somit bieten anonyme Netzwerke einen anonymen Kanal für die User. Die Daten werden in anonymen Netzwerken verschlüsselt. Anonyme Netzwerke sind die P2P-Netzwerke zwischen allen teilnehmenden Knoten[437]. Um die Anonymität herzustellen, werden alle Anfragen über zufällige Wege durch das P2P-Netzwerk geroutet. Auf dieser Weise wird jede Anfrage zufällig entweder direkt zum Empfänger oder über andere Nachbarknoten gesendet. Dadurch kann jeder Knoten abstreiten, der Initiator der Anfrage zu sein. Prominente Beispiele für die anonymen

---

435 Vgl. Ein Remailer ist ein Computerdienst, der die eMail entpersonalisiert. Ein Remailer ermöglicht es jemandem eine eMail zu schicken oder in eine Usenet-Newsgruppe zu posten, ohne daß der Empfänger den Namen oder die eMail-Adresse des Senders herausbekommt. Vgl. http://www.anon.gildemax.de/, Stand: 04.07.2009. Vgl. dazu auch mit den Erläuterungen im Abschnitt 4.3.1.1 Senderanonymität, S. 91. Für einen allgemeinen Überblick über Anonymous Remailers unter http://www.google.com/Top/Computers/Internet/E-mail/Anonymous_Mailers/. Ausführliche Informationen über Anonymus Remailers unter http://www.andrebacard.com/remail.html sowie http://www.emailprivacy.info/remailers, Stand: 04.07.2009.

436 Vgl. Goltzsch (2003), S. 114.

437 Knoten, auch Netzwerkknoten genannt, ist ein Netzwerkelement. Ein Netzwerkelement ist eine Bezeichnung für ein Gerät in einem Telekommunikationsnetz, z. B. Router, Server etc. Vgl. http://www.itwissen.info/definition/lexikon/Netzwerkelement-NE-network-element.html, Stand: 19. 01.2010.

Netzwerke sind die Konzepte von Crowds und TOR (The Onion Router)-Netzwerke.[438]

5.2.3 Anonyme Protokolle

Anonyme Protokolle (Anonymus Protocols oder auch Anonymus Subscription Services) erlauben Usern, sich für einen elektronischen Service anzumelden und diesen dann durch anonyme Zugriffe zu nutzen. Der Serviceprovider erfährt jedoch nicht, wer auf diesen Service zugreift bzw. zugegriffen hat. Darüber hinaus kann der Serviceprovider zwei Zugriffe nicht mit derselben Person verketten. Die Nutzung des Service ist nur den autorisierten Usern erlaubt. Außerdem erlaubt der Serviceprovider Usern nur eine bestimmte Zahl der Zugriffe auf die Dienste. Beispielsweise kann ein User nur 30 Zugriffe auf Dienste haben, für die er bezahlt hat.[439]

5.2.4 Anonymitätskonzepte

Es gibt derzeit eine Reihe von Methoden und Services für die Herstellung der Client-Anonymität, durch die User ihre Privatsphäre vor den Angreifern und Beobachtern schützen können. Daher sollen in diesem Kapitel diejenigen Konzepte von Anonymitätstechniken und die Anonymisierungsdienste für die Anonymität in stationären und mobilen Kommunikationsnetzen dargestellt werden, die gegenwärtig in der Literatur und Praxis existieren und von den Usern am meisten benutzt werden. Diese Anonymitätskonzepte und -techniken lassen sich wie folgt in drei Gruppen zusammenfassen:[440]

1. Proxies
2. Peer-to-Peer-Netzwerke (Crowds, mCrowds)
3. Mix-Netze

Im Folgenden werden die einzelnen Konzepte zur User-Anonymität in stationären und mobilen Kommunikationsnetzen und deren Anwendung in der Praxis erläutert:

---

[438] Das Konzept von Crowds und TOR-Netzwerke werden im Abschnitt 5.2.4 Anonymitätskonzepte, S. 124ff. näher erläutert.

[439] Vgl. Ramzan/Ruhl (2000), S. 1.

[440] Vgl. Federrath/Martius 1998), S. 3; Federrath/Pfitzmann (1998), S. 630; Köpsell/Federrath/Hansen (2003), S. 139.

5.2.4.1 Proxies und deren Anwendung in der Praxis

Eine der im Internet am häufigsten genutzten Anonymitätstechniken ist der Proxy oder Proxy Server. Das Wort Proxy bedeutet Stellvertreter und erledigt Aufgaben im Auftrag eines anderen.[441] Ein Proxy ist ein Programm, das sich auf einem Gateway[442] zwischen den Clients und einem anderen Set von Server, z. B. Webserver befindet und zwischen den Clients und dem Web-Server vermittelt. Der Computer, auf dem der Proxy-Service läuft, wird als Proxy-Server bezeichnet. Ein Client im lokalen Netwerk (LAN) fordert Webseiten nicht direkt vom ursprünglichen Server an, sondern vom Proxy-Server, der gegenüber dem Client wie einen Webserver funktioniert. Auf der anderen Seite holt der Proxy die Webseiten vom ursprünglichen Webserver im Internet. In diesem Fall ist der Proxy für den Webserver wie ein Client.[443] Dabei wird die IP-Adresse vom Client nicht dem Webserver im Internet vermittelt, sondern dem Proxy. Beim Webserver im Internet erscheint nur eine offizielle IP-Adresse vom Proxy-Server. Das gesamte Netzwerk von Clients befindet sich hinter dem Proxy-Server und bleibt für den kriminellen User verdeckt. Damit erreicht man eine bestimmte Anonymität. Der Proxy kontrolliert die Kommunikation und den Datenaustausch zwischen dem eigenem Netzwerk und dem Internet. In der Abbildung 18, S. 126 wird die Funktionsweise der Proxies dargestellt.

Ein Proxy ermöglicht es allen Clients in einem Netzwerk eine einzige Internetverbindung gleichzeitig zu nutzen. Das heißt, alle Clients verbinden sich gleichzeitig mit dem Internet über den Proxy. Dabei dient der Proxy als Firewall[444] und verhindert somit die unerwünschten Zugriffe auf das eigene Netzwerk aus dem Internet. Der Proxy speichert die angeforderten Webseiten in einem Proxy-Cache[445] und verwaltet

---

441 Vgl. Schemberg/Linten (2006), S. 100.

442 Gateway ermöglicht als Vermittlungscomputer die Kommunikation zwischen Rechnern, die in unterschiedlichen Datennetzen oder Datei-Diensten integriert sind. Vgl. http://woerterbuch.babylon.com/gateway, Stand: 29.01.2010.

443 Vgl. Schemberg/Linten(2006), S. 100.

444 Firewall ist eine Technik in Form von Hard- und/oder Software, die den Datenfluss zwischen einem privaten und einem ungeschützten Netzwerk (also LAN und Internet) kontrolliert bzw. ein internes Netz vor Angriffen aus dem Internet schützt. Dazu vergleicht eine Firewall z.B. die IP-Adresse des Rechners, von dem ein empfangenes Datenpaket stammt, mit einer Liste erlaubter Sender - nur deren Daten dürfen passieren. Vgl. http://woerterbuch.babylon.com/firewall, Stand: 29.01.2010.

445 Der Cache ist ein schneller Puffer, der Daten zwischenspeichert und diese immer wieder sehr schnell zur Verfügung stellen kann. Ein Cache enthält Kopien von Inhalten eines anderen (Hintergrund-)Speichers und beschleunigt somit den Zugriff darauf.

Fortsetzung auf der nächsten Seite

die Aktualität der Webseiten. Wenn der Client eine Webseite nochmals abruft, dann holt der Proxy die Webseite vom Proxy-Cache. Wenn sich die Website seit letztem Abruf verändert hat oder die Webseite dem Proxy noch nicht bekannt ist, dann holt der Proxy die neue Webseite entweder direkt vom ursprünglichen Web-Server, oder vom Parent-Proxy (Proxy-Server des Proxy-Servers) oder vom Sibling-Proxy (Geschwister-Proxy mit demselben Parent).[446] Informationen werden den Clients bei mehrmaligen Abrufen schneller geliefert. Damit wird der Internetverkehr entlastet.

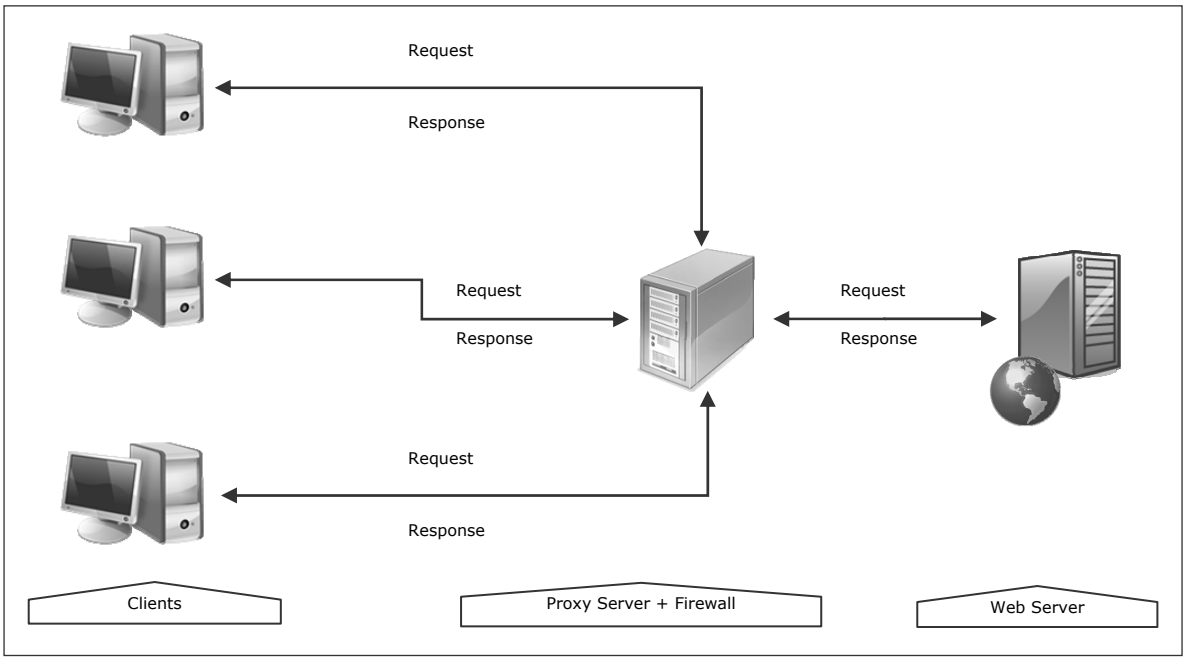

Abbildung 18: Funktionsweise der Proxies

Der Proxy-Server ist nicht nur aus Kostengründen vorteilhaft, bietet sondern auch den Clients kürzere Antwortzeiten. Der Client sendet Anfragen zum Server, der die Anfragen weiterverarbeitet und dem Client die Ergebnisse zurücksendet. Die Anonymität im Server liegt in der großen Anzahl von Nachrichten, welche von einem einzigen Proxy-Server gesendet werden. Ein Beobachter hat keinesfalls die Möglichkeit, zu bestimmen, wer die Urheber der Anfragen sind. Anonyme Proxies sind der einfachste Weg, um eine schnelle Basis-Anonymität herzustellen. Sie bieten dagegen wenig Schutz vor Angriffen von Dritten wie z. B. Spionage, Sabotage oder Phishing etc.

---

grund-)Speichers und beschleunigt somit den Zugriff darauf. Vgl. http://woerterbuch.babylon.com/cache, Stand: 29.01.2010.

446 Vgl. Schütz (2006), S. 9.

Die Proxies werden auch für die Anonymisierungsdienste im Internet benutzt, um die eigene IP-Adresse zu verschleiern und somit im Internet anonym surfen zu können. Wenn der User im Internet ungeschützt surft, gibt er die Webadresse im Webbrowser ein und ruft die Webseite oder bestimmte Webdienste ab. Die Anfrage wird zum Web-Server weitergeleitet, und von dort wird die angeforderte Information zum Client zurückgeschickt. Bei der Anfrage wird auch die IP-Adresse des Clients an den Web-Server übermittelt, damit der Web-Server die angeforderten Webseiten an den Client zurückschicken kann. Diese IP-Adresse wird mit weiteren Anfrageinformationen beim Web-Server in Protokollen (Logfiles)[447], gespeichert. Der Betreiber der Webseite kann die in den Logfiles gespeicherten Informationen sortieren und sie gegebenenfalls weiterverwenden. So können User identifiziert oder ihr Surfverhalten untersucht werden. Um dies zu verhindern, werden anonyme Proxies eingesetzt. Wenn der Client oder User einen anonymen Proxy-Server zwischen den eigenen Rechner und die zu besuchende Webseite schaltet, kann der Betreiber der Webseite nur die IP-Adresse des Proxy-Servers ermitteln, nicht aber die des Clients. Auf der anderen Seite können nur die Anfragen vom Client zum Proxy-Server zurückverfolgt werden, nicht jedoch die Zielwebserver. Wenn beim Proxy-Server die Logfiles von Clients gespeichert werden, können die Identität von Clients und die angeforderten Webseiten festgestellt werden.[448]

Im Internet kann man etliche Anonymisierungsdienste bzw. anonyme Proxies wie Anonymouse.org etc. nutzen.[449] Die Anonymisierungsdienste werden meistens von Universitäten, Behörden und manchmal auch von Privatpersonen angeboten. Der Anonymisierungsdienst von Anonymizer.com funktioniert mit dem Prinzip der Webbrowserkonfiguration und kann beispielsweise durch die Eingabe der IP-Adresse und des Port des Proxy-Servers in einer Webbrowserkonfiguration genutzt werden.[450] Der Anonymisierungsdienst von Anonymouse.org hingegen funktioniert mit dem formularbasierten Prinzip und kann über ein Webinterface genutzt werden, in dem man einfach die Webadresse eingibt.

---

[447] Logfile ist die englische Bezeichnung für Logdatei oder Protokolldatei und beinhaltet das automatisch erstellte Protokoll aller oder bestimmter Aktionen von Prozessen auf einem Computersystem. Vgl. http://www.itwissen.info/definition/lexikon/logfile-Log-Datei.html, Stand: 30.10.2009.

[448] Vgl. http://www.computerbetrug.de/anonym-surfen-im-internet/anonyme-proxy-server/, Stand: 30. 10.2009.

[449] Vgl. http://anonymouse.org/, Stand: 30.10.2009.

[450] Vgl. http://www.anonymizer.com/, Stand: 30.10.2009.

In der Abbildung 19 und der Abbildung 20 wird das Beispiel von Anonymouse.org veranschaulicht. In der Abbildung 19 sind die echten Client- bzw. Userdaten und -informationen wie die IP-Adresse, Host-Nummer und der Browsertyp und das Betriebssystem ohne die Nutzung des Anonymisierungsdienstes zu sehen. In der Abbildung 20 nutzt der User nun den Anonymisierungsdienst und verschleiert seine Daten und Informationen der ersten Tabelle. Der Zielwebserver oder ein Beobachter kann lediglich die IP-Adresse und Host-Nummer von Anonymouse.org sehen bzw. nicht sehen, wer die Webseiten tatsächlich abgerufen hat. Allerdings muss der User sich auf den Betreiber des Anonymisierungsdienstes verlassen können, dass die Proxy-Server tatsächlich anonym sind und deren Betreiber keine Informationen über die User sammeln.[451] Außerdem ist es nicht immer zuverlässig, dass die Proxy-Server die Anonymität der Clients bzw. User und die erforderliche Geschwindigkeit beim Surfen garantieren. Ein Nachteil bei der Verwendung der Proxies liegt auch darin, dass diese über ihre IP auch bestimmte Informationen senden, etwa eine Länderkennung. Es gibt durchaus Webseiten und Dienste, die Anfragen von IP-Adressen aus bestimmten Ländern unterbinden.[452]

IP	93.202.25.257
Host	port-93-202-25-257.dynamic.qsc.de
Browser & OS	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; InfoPath.1)

Abbildung 19: Client- bzw. Userdaten und -informationen

IP	193.200.150.26
Host	anonymouse.org
Browser & OS	http://Anonymouse.org/ (Unix)

Abbildung 20: Anonymes Surfen im Internet über Anonymouse.org[453]

[451] Vgl. Federrath/Martius (1998), S. 93.

[452] Vgl. http://www.computerbetrug.de/anonym-surfen-im-internet/anonyme-proxy-server/, Stand: 30. 10.2009.

[453] Vgl. http://anonymouse.org/, Stand: 30.10.2009.

Bei dieser Anonymisierungstechnik ist eine Beobachtung und Verkettung von Informationen durch einen Angreifer bzw. Beobachter möglich. Ein Angreifer kann beispielsweise diese Informationen im Netz abhören und Verkehrsanalysen durchführen. Somit ist diese Anonymisierungstechnik nicht sicher. Die Verschlüsselung zwischen Webbrowser und Proxy verhindert zwar die Verkettbarkeit der Anfragen über das Aussehen der Informationen, nicht jedoch über die Länge und Zeit dieser Informationen.[454]

5.2.4.2 Crowds und deren Anwendung in der Praxis

Eine weitere Möglichkeit zur Anonymität ist das Konzept von Crowds, das anonymes Surfen im Internet ermöglicht. Das Konzept von Crowds wurde 1997 von Michael K. Reiter und Aviel D. Rubin entwickelt. Die Grundidee vom Konzept ist die Mischung der Aktionen von einem User in eine Menge der Aktionen anderer User. Diese Menge wird als „Crowd“ bezeichnet und entsteht durch die Ansammlung von Usern zu großen und geographisch unterschiedlichen Gruppen.[455]

Nach dem Konzept stellt ein User eine Verbindung zu einer Crowd vorhandener Clients bzw. User her und führt alle seine Netzwerkanfragen über diese Crowd aus. Die verbundenen Webserver können die Identität der Clients nicht feststellen, da die Netwerkanfragen von irgendeinem User in der Crowd stammen. Die Clients bzw. User der Crowd bleiben somit anonym. Auch die miteinander kooperierenden User innerhalb der Crowd können nicht herausfinden, wer die Anfrage bzw. Nachricht ursprünglich geschickt hat.[456] Jeder User ist durch einen Prozess auf seinem Rechner dargestellt und wird als *Jondo*[457] bezeichnet. Ein Jondo ist ein Prozess, der auf dem Rechner des Users läuft. Nach dem der Jondo gestartet wurde, wird ein Kontakt zu einem Server in der Crowd hergestellt, der als *Blender* bezeichnet wird und für die Zugangskontrolle der User in die Crowd zuständig ist, damit der User in die Crowd aufgenommen wird. Sobald der Blender die Teilnahme an der Crowd bestätigt hat, informiert er den Jondo und andere User über die Teilnahme an der Crowd. Der User

---

454 Vgl. Federrath/Martius (1998), S. 93.

455 Vgl. Reiter/Rubin (1997), S. 1.

456 Vgl. Reiter/Rubin (1997), S. 7.

457 Als Jondo bezeichnen Reiter und Rubin den anonym übermittelten User in der Crowd. Das Jondo ist aus dem Namen „John Doe“ kreiert. Vgl. Reiter/Rubin (1997), S. 7.

wählt diesen Jondo-Prozess als seinen lokalen Proxy-Server und konfiguriert in seinem Webbrowser seinen Host[458] und Port[459]-Namen für alle Netzwerkanfragen.

Wenn ein User eine erste Anfrage einer Webseite erhält, startet der Jondo des Users damit, einen zufälligen Pfad von Jondos zu bilden, über den die Netzwerktransaktionen zum und vom Ziel-Web-Server ablaufen sollen. Der Jondo des Users wählt zufällig einen Jondo unter den verfügbaren Jondos innerhalb der Crowd (die Wahl des eigenen Jondos ist auch möglich) aus und leitet ihm die Anfrage weiter. Wenn der gewählte Jondo die Anfrage erhält, führt dieser die Anfrage entweder aus oder leitet diese Anfrage zu einem anderen zufällig gewählten Jondo weiter. Diese Anfrage läuft unter den Jondos so lange zufällig durch, bis diese von einem Jondo ausgeführt ist und die Antwort vom Ziel-Web-Server entlang der Jondo-Kette zurück gesendet wird. Der Empfänger dieser Antwort kann die Identität vom Urheber nicht feststellen. Es ist ebenso wahrscheinlich, dass die Anfrage tatsächlich vom Urheber weitergeleitet ist.

In der Abbildung 21, S. 131 wird die Kommunikation der Jondos mit den Ziel-Web-Servern über die möglichen Pfade dargestellt.[460] Jeder Kommunikationspfad zwischen dem Initiator und dem Ziel-Web-Server ist mit gleichen Linien gezeichnet. In diesem Beispiel sind es die Pfade

1 → 5 → Server 1;

2 → 6 → 2 → Server;

3 → 1 → 6 → Server;

4 → 4 → Server;

5 → 4 → 6 → Server;

---

[458] Hosts sind Großrechner und Server , an denen Arbeitsstationen angeschlossen sind, für die innerhalb eines Netzwerks besondere Dienste bereitgestellt werden: einige Hosts sind z. B. News-, FTP- oder Name-Server, andere sind Router oder HTTP-Server, die das "Hypertext Transfer Protocol" bereitstellen, auf dem das World Wide Web basiert.
Vgl. http://woerterbuch.babylon.com/host, Stand: 30.10.2009.

[459] Verbindungsmöglichkeit des PCs mit Peripheriegeräten. TCP/IP-Anwendungen adressieren den Kommunikationspartner zum einen über die IP-Adresse, zum anderen über eine-Port-Nummer, die den Dienst auf dem Zielrechner spezifiziert. Dafür gibt es sogenannte well known ports, für FTP ist dies beispielsweise die Nummer 21, für HTTP (WWW) 80. Vgl. http://woerterbuch.babylon.com/host, Stand: 30.10.2009.

[460] Vgl. Ebenda.

und 6 → 3 → Server.

Die Kommunikationspfade zwischen dem Initiator und Ziel-Web-Server werden so lange genutzt, bis der Initiator eine Antwort erhält. Bei einer Anfrage neuer Webseiten wird ein neuer Kommunikationspfad hergestellt. Die Kommunikation zwischen den Jondos ist nach dem symmetrischen Krypto-Verfahren verschlüsselt. Die paarweise verteilten symmetrischen Schlüssel sind nur zwei der Jondos bekannt. Die Krypto-Schlüssel werden vom Blender, der neben der Registrierung von Jondos auch für die Verteilung von symmetrischen Krypto-Schlüsseln in der Crowd zuständig ist, verteilt, wenn die Jondos an der Crowd teilnehmen.

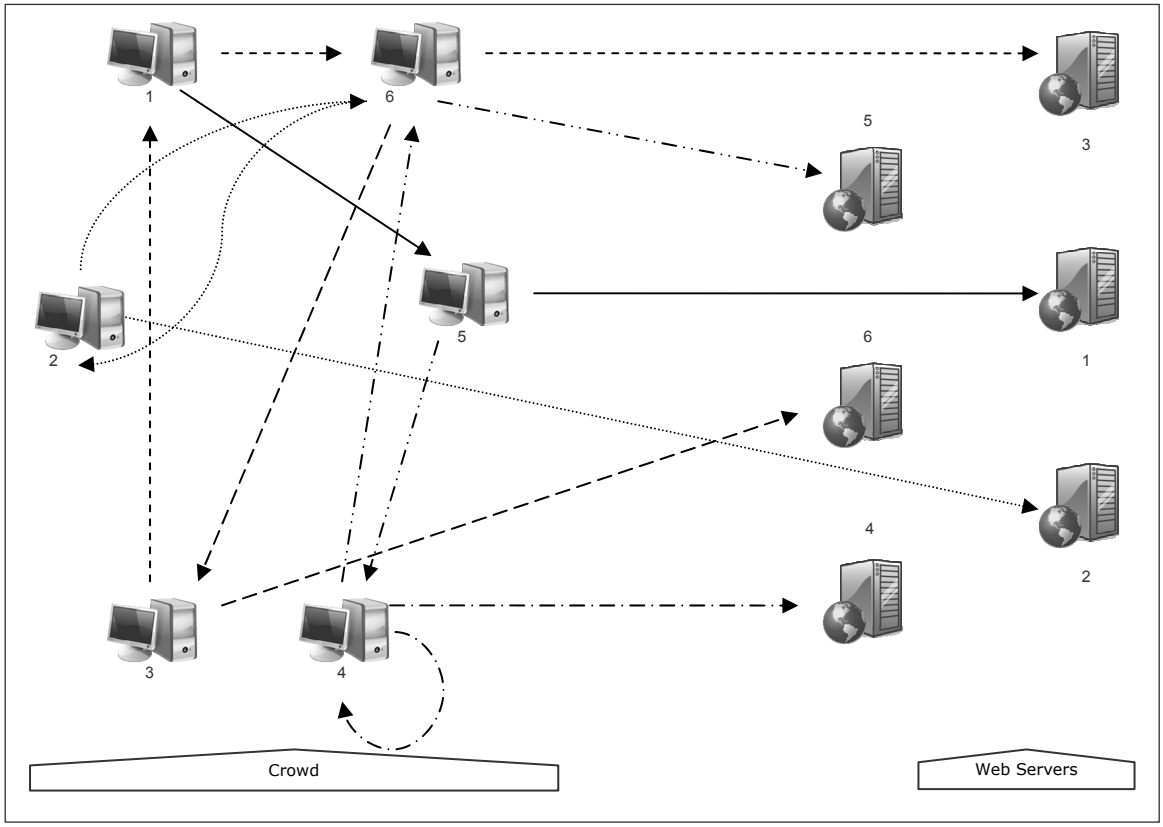

Abbildung 21: Die Kommunikation über mögliche Pfade innerhalb einer Crowd[461]

Für die Teilnahme an der Crowd muss der User einen Account beim Blender einrichten. Der User kreiert einen Accountnamen und ein Passwort. Wenn der Jondo des Users einen neuen Prozess startet, benutzen Jondo und Blender das Passwort für die gegenseitige Authentifizierung der Kommunikation. Wenn der Blender den Jondo in die Crowd aufnimmt, speichert er dann den neuen User mit seiner IP-

[461] Vgl. Reiter/Rubin (1997), S. 8.

Adresse, Port-Nummer und dem Accountnamen in die Crowd-Liste anderer Jondos. Danach informiert der Blender alle Jondos über den neuen Jondo. Dabei erzeugt der Blender eine neue Liste der zugeteilten Krypto-Schlüsseln und verteilt diese an die Jondos für die gegenseitige Authentifizierung. Jeder Jondo erhält vom Blender immer eine aktualisierte Liste von Jondos in der Crowd, wenn ein neuer Jondo in der Crowd aufgenommen bzw. gelöscht wird. Jeder Jondo pflegt eine eigene Mitgliederliste und kann für die Sicherheit Mitglieder (Jondos) der Crowd aus der eigenen Liste entfernen, wenn diese fehlschlagen.

5.2.4.3 mCrowds und deren Anwendung in der Praxis

Das Konzept mCrowds ist eine Erweiterung des Konzeptes Crowds für mobile Anwendungen und an der Universität Karlstadt in Schweden entwickelt.[462] Das Konzept mCrowds ermöglicht anonymes Surfen mit WAP-fähigen Mobilfunkgeräten wie WAP-Handys und gewährleistet die Anonymität von Usern im mobilen Internet. mCrowds kann beispielsweise bei Location based und context awareness services eingesetzt werden, um die Weitergabe von personenbezogenen Daten und Informationen an den Service Provider minimieren zu können.

Die Technologie mCrowds verwendet in mobilen Umgebungen eine Erweiterung des originalen Kommunikationsprotokolls, das in Crowds im Internet benutzt wird. Um mCrowds zu benutzen, installiert ein User mCrowds auf sein Mobilfunkgerät und konfiguriert diese. Nach der Registrierung beim „Blender“ nimmt der mobile User an der Crowds teil und kann dann im mobilen Internet anonym kommunizieren. Dabei muss der mobile User seine eigene Identität zum End-Server wie im konventionellen Internet nicht preisgeben. Auch wenn sich einige Bedingungen während der Aktion des originalen Kommunikationsprotokolls zu mobiler Umgebung geändert haben, liefert mCrowds die gleichen Anonymitätseigenschaften wie das konventionelle Crowds-System. Zu einer Crowd können sowohl konventionelle Internetuser als auch mobile User gehören.

Die mCrowds-Applikation ist in der Programmiersprache Java entwickelt worden und deshalb plattformunabhängig. Die Jondo-Applikation vom mobilen User funktioniert wie ein Local proxy server (Privacy Proxy oder WAP-Proxy) auf einem stationären PC vom User oder TTP. In der Abbildung 22, S. 133 wird eine anonyme mobile

[462] Vgl. Andersson/Fischer-Hübner/Lundin (2003), S. 79ff; Andersson/Lundin/Fischer-Hübner (2004), S.1ff.

Kommunikation durch die Nutzung von mCrowds dargestellt. Der Privacy proxy oder WAP-Proxy ist eine Schnittstelle für die vertraulichen, personenbezogenen Daten und Informationen. Es wird daher empfohlen, dass die WAP-Proxy entweder unter Kontrolle vom User oder TTP sein sollte.[463]

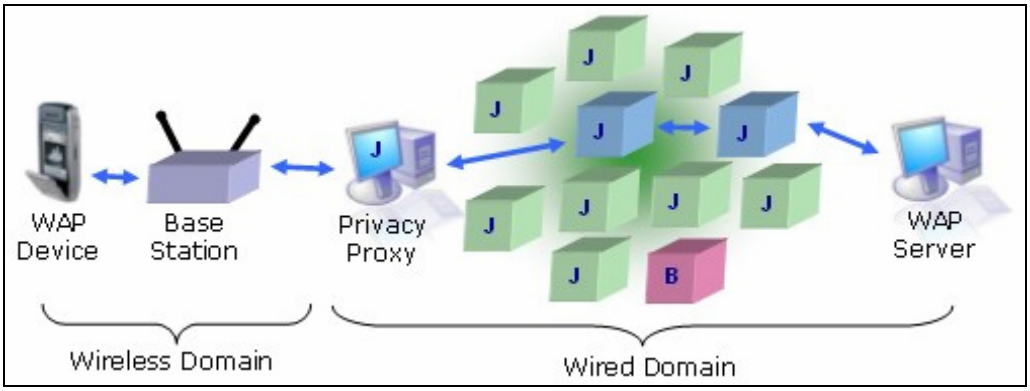

Abbildung 22: Funktionsweise von mCrowds[464]

Das Konzept mCrowds ist auf seiner Leistung hin theoretisch getestet worden.[465] Außerdem bietet das Konzept mCrowds eine Anonymität in mobilen Umgebungen für die mobilen User. Dem Konzept fehlen zwar praxisrelevante Erfahrungen, jedoch dürfte der Bedarf an den Applikationen, die die User-Anonymität in mobilen Umgebungen gewährleisten, im Zuge der Entwicklungen im Bereich mobiler Anwendungen und Dienste steigen. Daher soll das Konzept mCrowds erst in der Praxis seiner Tauglichkeit hin geprüft werden.

5.2.4.4 Mixe und deren Anwendung in der Praxis

Das Konzept der Mixe wurde 1981 von David Chaum entwickelt.[466] Die umkodierenden Mixe werden zur Anonymität und Unbeobachtbarkeit in Vermittlungsnetzen eingesetzt. Nach dem Konzept der Mixe wird die Kommunikationsbeziehung zwischen dem Sender und Empfänger verborgen und somit in Email-Kommunikation

---

[463] Vgl. Andersson/Fischer-Hübner/Lundin (2003), S. 89.

[464] Vgl. Ausführliche Informationen finden sich unter dem Projektportal FIDIS: http://www.fidis.net/resources/deliverables/hightechid/int-d3300/doc/24/, Stand: 31.10.2009.

[465] Vgl. Ausführliche Informationen finden sich unter dem Projektportal FIDIS: http://www.fidis.net/resources/deliverables/hightechid/int-d3300/doc/24/, Stand: 02.11.2009.

[466] Vgl. Chaum (1981).

und WWW eine „starke Anonymität“ gewährleistet, die nicht von einem einzigen Betreiber abhängig ist.[467]

Die Nachrichten von Sendern werden nicht direkt an den Empfänger, sondern über die hintereinander geschalteten Mixe, die jeweils von unabhängigen Betreibern betrieben werden, geschickt. Ein Mix speichert die eingehenden Nachrichten von mehreren Sendern. Diese Nachrichten werden, wie in der Abbildung 23, S. 135 dargestellt wird, umkodiert, um ihr Aussehen zu verändern. Dann werden die Nachrichten umsortiert, um die Reihenfolge der ausgehenden Nachrichten zu verändern. Um Angriffe durch wiederholtes Senden gleicher Nachrichten zu verhindern, prüft der Mix, ob die Nachrichten bereits gemixt worden sind und lehnt sie gegebenenfalls ab. Da ein Mix die Nachricht deterministisch umkodiert, würde eine Wiederholung gleicher Nachrichten zur Ausgabe der gleichen umkodierten Nachricht führen. Somit wären eine Verkettung von eingehenden und ausgehenden Nachrichten und eine Enthüllung einer Kommunikationsbeziehung möglich. Um die Verkettung von eingehenden und ausgehenden Nachrichten durch einen Beobachter zu verhindern, haben alle Nachrichten die gleiche Länge.[468]

Da eine Nachricht nur innerhalb eines Schubs anonym ist, muss sichergestellt sein, dass ein Angreifer nie alle Nachrichten außer einer Nachricht selbst erzeugt haben darf. Andernfalls würde das die Aufdeckung der Kommunikationsbeziehung bedeuten. Die Kommunikationsbeziehung zwischen Sendern und Empfängern bleibt für alle Außenstehenden, Mixbetreiber und Netzbetreiber unbeobachtbar. Erst wenn alle an einer Kommunikationsbeziehung beteiligten Mixe zusammenarbeiten würden, wäre eine Aufdeckung einer Kommunikationsbeziehung ebenfalls möglich.[469]

Um eine Zuordnung von Sender und Empfänger einer Nachricht zu erschweren, müssen alle Sender zu jedem Zeitpunkt eine Nachricht senden und auch alle Empfänger genau eine Nachricht empfangen. Falls sich die Kommunikationsbeziehung nur auf aktive Teilnehmer beschränkt, müssen auch passive Teilnehmer künstlich erzeugte leere Nachrichten (Dummy Traffic) senden, damit die Teilnehmer-

---

467 Vgl. Federrath (2003), S. 172; Schwark (2004), S. 28.

468 Vgl. Federrath (2003), S. 172ff; Federrath/Martius (1998), S. 94; Federrath/Pfitzmann (1998), S. 629.

469 Vgl. Ebenda.

gruppe gleich groß bleibt und die Unbeobachtbarkeit des Einzelnen nicht sinkt. Der letzte Mix erkennt die Leernachrichten und sortiert sie aus.[470]

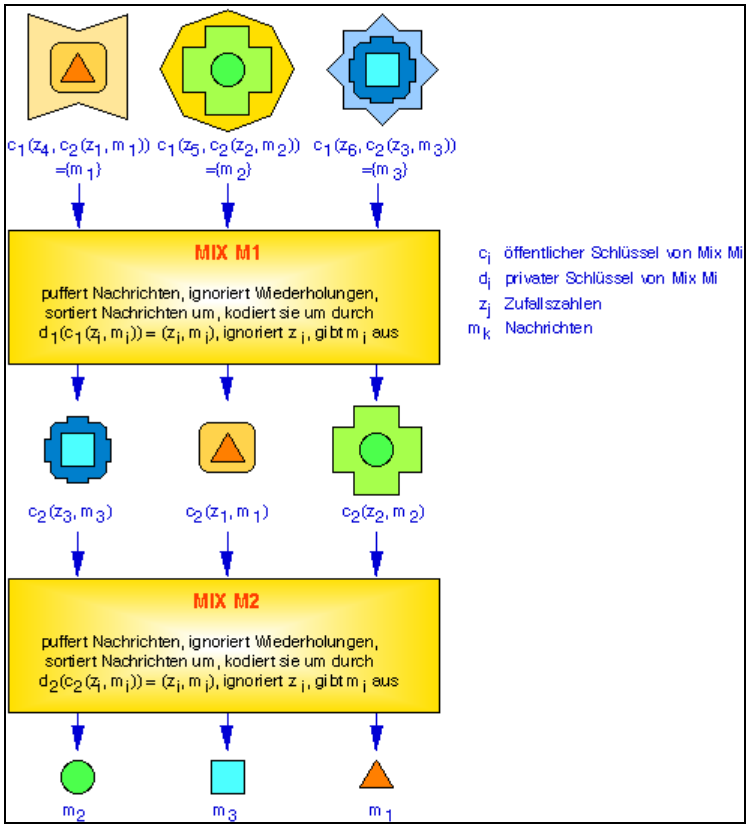

Abbildung 23: Umkodieren zu mixender Nachrichten[471]

Die Grundidee eines Mixes ist das Umkodieren von Nachrichten nach dem asymmetrischen Verschlüsselungs- und Entschlüsselungsverfahren. Die Nachrichten werden mit dem privaten Schlüssel des Mixes entschlüsselt, d.h. umkodiert und an den nächsten Mix weitergeschickt. Der Verschlüsselungsschlüssel (Public Key) ist öffentlich bekannt, jeder kann eine Nachricht für den Empfänger verschlüsseln. Der Entschlüsselungsschlüssel (Private Key) ist nur dem nächstliegenden Mix bekannt. So kann dieser Mix die eingehenden Nachrichten entschlüsseln. Folglich kennt der erste Mix zwar den Sender der verschlüsselten Nachricht, erfährt jedoch weder etwas über den Empfänger noch über den Inhalt der Nachricht. Der letzte Mix kennt den Empfänger einer Nachricht, kann aber über den Sender nichts erfahren. Mittlere Mixe kennen nur den Vorgänger-Mix und den Nachfolger-Mix. Somit ist die Sender-

[470] Vgl. Ebenda.

[471] Vgl. Federrath/Martius (1998), S. 94.

anonymität gewährleistet. Die Unbeobachtbarkeit der Kommunikationsbeziehungen können durch diverse unabhängige Betreiber der zwischengeschalteten Mixe gewährleistet werden, solange mindestens einer der Mixe vertrauenswürdig ist.[472]

Für die anonyme Internetnutzung über die Mix-Netze wurden verschiedene Systeme entwickelt und existieren gegenwärtig verschiedene Anonymisierungsdienste in der Praxis. Eine dieser Anonymisierungsdienste ist das AN.ON bzw. JAP-Projekt, das in der Praxis sehr bekannt ist und von den meisten Usern benutzt wird.

Das Projekt AN.ON und JAP: Der JAP (Java Anon Proxy) ist ein Anonymisierer[473] zum anonymen und unbeobachtbaren Surfen im Internet, der im Rahmen des Projektes AN.ON[474] der Technischen Universität Dresden mit den Projektpartnern Universität Regensburg und Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein entwickelt wurde. Die kommerzielle Weiterentwicklung von JAP wird unter dem Namen JonDonym durch die JonDos GmbH[475] geführt.

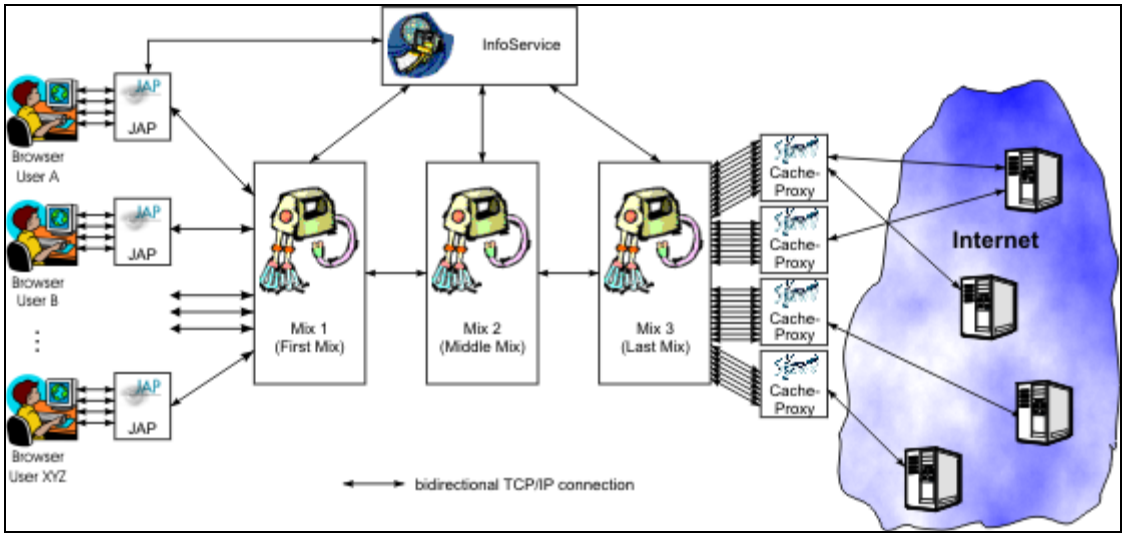

Abbildung 24: JAP Architektur und Funktionsweise[476]

---

472 Vgl. Federrath/Martius (1998), S. 94ff; Federrath/Pfitzmann (1998), S. 629; Schwark (2004), S. 28.

473 Der Begriff Anonymisierer (engl. anonymizer) wird definiert als ein System, das als ein Proxy zwischen User und Zielserver geschaltet wird, um die Anonymität von Usern im Internet zu bewahren. Vgl. http://woerterbuch.babylon.com/Anonymisierer, Stand: 06.01.2009.

474 Ausführliche Informationen über das Projekt „AN.ON - Starke Unbeobachtbarkeit und Anonymität im Internet“ unter http://anon.inf.tu-dresden.de/ sowie https://www.datenschutzzentrum.de/projekte/anon/, Stand: 06.01.2009.

475 Vgl. Ausführliche Informationen finden sich unter https://www.jondos.de/de/, Stand: 06.01.2009.

476 Vgl. Ausführliche Informationen finden sich unter http://anon.inf.tu-dresden.de/desc/desc_anon.html, Stand: 05.11.2009.

Der JAP ist eine Proxy-Server-Software, die durch den Einsatz eines Mix-Proxys das Nutzerverhalten von Internetusern größtenteils verwischt. Die User können mit JAP anonym und unbeobachtbar durch das Internet surfen und eigene Surfspuren im Internet verwischen. Weder der angefragte Server oder ein Beobachter kann herausbekommen, wer welche Seite aufgerufen hat. Die JAP-Software schließt den User mit vielen anderen Internetnutzern zu einer so genannten Mix-Proxy-Kaskade zusammen, wie in der Abbildung 24, S. 136 dargestellt wird. Dadurch werden Internetanfragen jedes Users unter den Anfragen von anderen Usern versteckt. Die Internetanfragen werden nicht direkt zum Ziel-Webserver, sondern über die Mix-Proxy-Kaskade geführt. An einer regulären Proxy-Kaskade sind mindestens drei Mix-Proxies beteiligt. So soll die Rückverfolgung einer Internetanfrage verhindert werden und ein User von JAP nicht aufgedeckt werden. Die unabhängigen Betreiber dieser Mixe sollen für die Vertrauensbildung ins System in einer Selbstverpflichtung erklären, dass sie weder Logfiles von Internetusern speichern noch mit den anderen Mix-Betreibern Daten austauschen.[477]

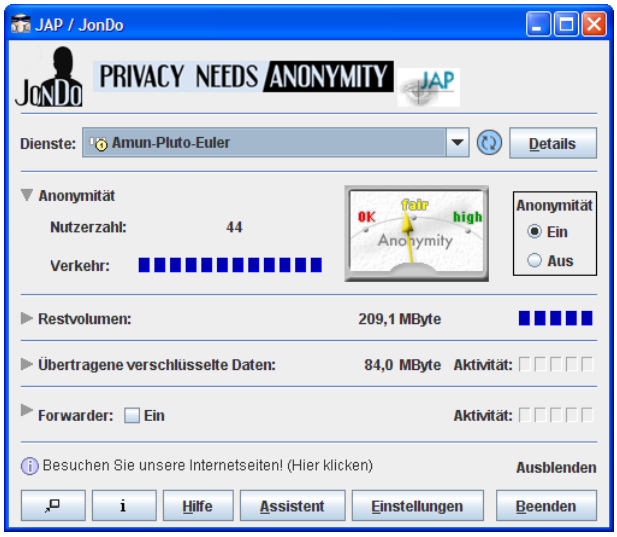

Abbildung 25: JAP-Software[478]

In der Abbildung 25 wird die JAP-Software dargestellt. Nach der Installation bzw. Konfiguration der JAP-Software wählt der User einen Anonymitätsservice in der Liste der Dienste auf der Software. Dann schaltet er die gewünschten Optionen der JAP-Software ein. Der User kann seine Anonymität während der Aktivität im Internet be-

[477] Vgl. JAP (2001), S. 1ff.

[478] Vgl. Ausführliche Informationen finden sich unter http://anon.inf.tu-dresden.de/screenshot.html, Stand: 07.01.2009.

obachten bzw. kontrollieren. Die JAP-Software bietet Internetusern die Möglichkeit zum Selbstschutz gegen professionelle Datensammler und Firmen, die Userprofile herstellen und weiterverkaufen. Da das JAP-System weiterentwickelt wird, soll das System letztlich auch gegen Angreifer schützen, die das gesamte Kommunikationsnetzwerk über langen Zeitraum überwachen und Kommunikationsverkehrsanalysen durchführen.[479] Während das JAP-System User gegen einen lokalen Angreifer und die Betreiber eines Mixes schützt, zeigt das System noch einige Schwächen. Gegen einen Angreifer, der das gesamte Internet überwacht oder den ersten und letzten Mix kontrolliert, kann das System noch nicht schützen. Außerdem darf ein Mix der Kaskade nicht mit dem Angreifer zusammenarbeiten.[480]

5.2.4.5 Onion Routing und dessen Anwendung in der Praxis

Eine andere Möglichkeit für die Anonymität ist das sog. Onion Routing. Onion Routing ermöglicht eine private Kommunikation über die öffentlichen Netzwerke durch eine Zahl von Knotenpunkten, sog. „onion routers“. Das wird als TOR (The Onion Router) bezeichnet, welches wiederum eine Implementation von Onion Routing ist. Die Nachrichten werden unter den Endusern als verschlüsselte „data onions“ durch einen zufälligen Pfad der vermittelnden Onion Routers gesendet. Die Userdaten werden mehrmals durch die Verwendung von öffentlichen Schlüsseln (Public Keys) der Server durch die für die Nachricht geplante Route verschlüsselt.[481]

Die Schichten werden mit Hilfe der privaten Schlüssel (Private Key) von einem Knotenpunkt zum anderen durch die ganze Route abgeschält. Die Nachricht wird dann entschlüsselt zum User geschickt. Bei jedem Schritt im Pfad der Nachricht kennt der Router nur die Identität vom vorhergehenden Router und vom Router, an den die Nachricht weitergeleitet werden muss. Wenn dies passiert ist, wird die gleiche Route für die Übertragung einer Zahl von Nachrichten genutzt, um die Effizienz eine Periode lang zu erhöhen. Die Route wird danach eingestellt, um mögliche Beobachter zu verhindern, die den Nachrichtenverkehr analysieren. Onion Routing ermöglicht gleichzeitig dem Sender einer Nachricht auch ein sog. „Reply Onion“ zu kreieren, der einen Pfad vom Empfänger enthält, um zurückzusenden.

---

[479] Vgl. JAP (2001), S. 1ff.

[480] Vgl. Ausführliche Informationen finden sich unter der Rubrik „Schwächen von JAP“ unter http://anon.inf.tu-dresden.de/desc/desc_anon.html, Stand: 07.01.2009.

[481] Vgl. https://www.torproject.org/, Stand: 07.01.2009.

TOR: Ein weit verbreiteter Anonymisierungsdienst in der Praxis ist das Softwareprojekt TOR (The Onion Router). TOR basiert auf dem Prinzip des Onion Routings und hat das Ziel, Internetuser gegen die Analyse der Verbindungsdaten durch Beobachter zu schützen und somit die Anonymität von Kommunikationspartnern im Internet zu gewährleisten. Das Prinzip Onion Routing basiert wiederum auf Chaum's Mix-Modell. Die Internetanfragen werden nicht direkt vom Sender zum Empfänger, sondern im TOR-Netzwerk über eine zufällige Route über mehrere Server geschickt. Ein Beobachter kann nicht sagen, woher die Internetanfrage stammt und wohin sie geschickt wird. Um TOR zu benutzen, muss der User die Software TOR auf seinem Rechner installieren. Die Software baut eine verschlüsselte Verbindung mit einem der im TOR-Netzwerk verfügbaren Servern (Torknoten) auf. Danach wird die Verbindung schrittweise über die zufällig gewählte Route erweitert und ein Kreis gebildet. Jeder Knoten kennt entlang der Route nur, wer Vorgänger-Knoten war und Nachfolger-Knoten ist. Kein Knoten kennt jemals die gesamte Route.[482]

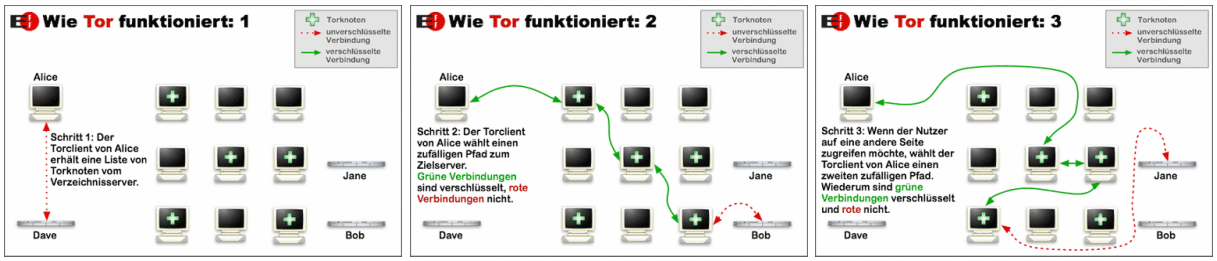

Abbildung 26: TOR Funktionsweise[483]

Wie in der Abbildung 26 dargestellt wird, werden für eine Route jeweils drei Server (Knoten) ausgewählt, um eine minimale Anonymität zu erreichen. Jede Route dauert eine Minute. Danach wechselt die Route. Die Nachrichten werden verschlüsselt. Auch wenn zwei Knoten einer Route manipuliert wurden und mindestens ein Knoten vertrauenswürdig bleibt, kann ein Beobachter die Nachrichten nicht mitlesen. Dadurch wird die Anonymisierung der Kommunikation gewährleistet. Der Ziel-Webserver kann nur die IP-Adresse des letzten TOR-Knotens der Route sehen. Der ursprüngliche User bleibt somit anonym.[484]

---

482 Vgl. Ausführliche Informationen finden sich unter http://www.torproject.org/overview.html.de, Stand: 07.01.2009.

483 Vgl. Ausführliche Informationen finden sich unter http://www.torproject.org/overview.html.de, Stand: 05.11.2009.

484 Vgl. http://www.torproject.org/overview.html.de und unter http://wiki.privacyfoundation.de/TOR%20Onion%20Router, Stand: 07.01.2009.

Derzeit besteht das TOR-Netzwerk aus ca. 2000 Servern, die weltweit verteilt sind. Ein Onion Router kann auch für andere Anwendungen, beispielsweise für Instant Messaging[485], IRC[486], E-Mail, P2P etc. genutzt werden. Dabei bietet TOR auch so genannte Hidden Services, um die Aufenthaltsorte der User zu verbergen. Außerdem können andere TOR-User so genannte TOR "Rendezvouspunkte" verwenden, um Hidden Services zu nutzen, ohne dabei die Netzwerkidentität des Anderen zu kennen.[487]

5.3 Regulatorische Rahmenbedingungen der Anonymität

Neben den organisatorischen und technischen Rahmenbedingungen spielen auch die regulatorischen Rahmenbedingungen für die Gestaltung der User-Anonymität eine entscheidende Rolle. Darunter fallen die strafrechtlichen Aspekte des Datenschutzes bzw. der Anonymität des Users, die in diesem Abschnitt näher erläutert werden. Unter Datenschutz wird der Schutz personenbezogener Daten vor Manipulation oder kriminellen Eingriffen verstanden. In erster Linie werden die natürlichen Personen, deren Daten verarbeitet werden, geschützt. Rechtliche Grundlage für den Schutz personenbezogener Daten ist das Grundrecht auf informationelle Selbstbestimmung. Danach soll jede Person bestimmen können, was mit ihren personenbezogenen Daten geschieht, wer welche dieser Daten sammelt, speichert und auswertet.[488] Dabei gibt es zwei grundsätzliche Bestimmungen im Datenschutz:

- das Verbotsprinzip mit Erlaubnisvorbehalt: Damit wird die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten verboten. Dieses Verbot findet keine Anwendung, soweit das Gesetz die Erhebung der Daten erlaubt oder die betroffene Person zustimmt, dass ihre persönlichen Daten erhoben, verarbeitet und genutzt werden dürfen.

---

485 Vgl. mit der Fußnote 192, S. 50.

486 Internet Relay Chat bezeichnet ein rein textbasiertes Chat-System. Es ermöglicht Gesprächsrunden mit einer beliebigen Anzahl von Teilnehmern in so genannten Channels. Neue Channel können üblicherweise jederzeit von jedem Teilnehmer frei eröffnet werden, ebenso kann man gleichzeitig an mehreren Channels teilnehmen. Beispiel: Hottub, http://www.itwissen.info/-definition/lexi-kon/Internet-relay-chat-IRC.html, Stand: 20.01.2010.

487 Vgl. Ausführliche Informationen finden sich unter http://www.torproject.org/overview.html.de und unter http://wiki.privacyfoundation.de/TOR%20Onion%20Router, Stand: 07.01.2009.

488 Vgl. Ausführliche Informationen finden sich unter http://www.datenschutz.de/recht/fundament/datenschutz/, Stand: 10.09.2009.

- der Grundsatz der Datenvermeidung und Datensparsamkeit: Mit diesem Grundsatz bezweckt man, dass man bei der Datenverarbeitung keine oder möglichst wenige personenbezogene Daten verwenden soll.

Neben diesen grundsätzlichen Datenschutzbestimmungen gibt es für den Datenschutz sowie für die Anonymität der User übergreifende Gesetze, Verordnungen, Regelungen und Richtlinien sowohl in Deutschland als auch in der EU. Dieser gesetzliche Rahmen bezieht sich hauptsächlich auf personenbezogene Daten einer natürlichen Person bestimmt.

In der BRD ist der Datenschutz in dem sog. Recht auf informationelle Selbstbestimmung verankert. Es wird aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 GG i. V. m. Art 1. Abs. 1 GG) abgeleitet. Nach der Rechtsprechung des Bundesverfassungsgerichts handelt es sich hierbei um ein sog. Datenschutzgrundrecht. Es ist aber im Grundgesetz selbst nicht niedergelegt. Das Recht auf informationelle Selbstbestimmung umfasst insoweit die Befugnis des Einzelnen grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen.[489]

In der EU sind die Mindeststandards für den Datenschutz der Mitgliedsstaaten mit der Richtlinie 95/46/EG (Datenschutzrichtlinie)[490] durch das Europäische Parlament und den Europäischen Rat bestimmt. Diese Richtlinie ist in der BRD erst im Jahr 2001 mit dem Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze in nationales Recht umgesetzt worden. In der Bundesrepublik gelten (allgemeine und spezielle) verschiedene/mehrere Gesetze (und Verordnungen) wie etwa das Bundesdatenschutzgesetz (BDSG), die Landesdatenschutzgesetze, das Telekommunikationsgesetz (TKG) und das Telemediengesetz (TMG). Neben den allgemeinen Gesetzen gelten spezielle Verordnungen wie die Telekommunikations-Überwachungsverordnung (TKÜV) etc. Diese Gesetze und Verordnungen regeln den Umgang mit Daten aller Art, die in den IT-Systemen und manuell verarbeitet werden.

---

[489] Vgl. mit den Erläuterungen über „Das Recht auf informationelle Selbstbestimmung“ unter http://www.mediaculture-online.de/Informationelle-Selbstbestimmu.944.0.html, Stand: 28.02.2010.

[490] Vgl. Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Ausführliche Informationen finden sich unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:NOT, Stand: 07.07.2009.

5.3.1 Gesetzliche Grundlagen zur User-Anonymität

Die gesetzlichen Grundlagen zur User-Anonymität sind in Deutschland im Bundesdatenschutzgesetz (BDSG) und den Landesdatenschutzgesetzen verankert. Im Folgenden werden diese gesetzlichen Grundlagen zur User-Anonymität erläutert.

5.3.1.1 Bundesdatenschutzgesetz und Landesdatenschutzgesetze

Das deutsche Bundesdatenschutzgesetz bestimmt zusammen mit den Datenschutzgesetzen der Länder und anderen bereichsspezifischeren Satzungen den gesetzlichen Rahmen für den Umgang mit personenbezogenen Daten. Landesdatenschutzgesetze sind die landesrechtlichen Gegenstücke in den 16 Bundesländern zum Bundesdatenschutzgesetz.[491]

Der Anwendungsbereich des BDSG bezieht sich auf den Umgang mit den personenbezogenen Daten und damit zusammenhängenden Aktivitäten wie Datenerhebung, Datenverarbeitung und -nutzung. Unter Datenerhebung versteht man das Beschaffen der Daten. Unter Datenverarbeitung versteht man das Speichern, Verändern, Übermitteln, Sperren und Löschen der Daten. Unter Datennutzung versteht man die Verwendung von Daten. Das BDSG regelt auch die Rechte und Pflichten der öffentlichen Stellen (Aufsichtsbehörden) und nicht-öffentlichen Stellen (privaten Unternehmen) für den Datenschutz, wie sie diese Daten für ihre Zwecke verarbeiten und nutzen dürfen. Der Zweck des BDSG ist in § 1 Absatz 1 BDSG definiert:

„Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.“

In § 3a BDSG spricht der Gesetzgeber von der „*Datenvermeidung und Datensparsamkeit“* und regelt, wie die Datenverarbeitungssysteme gestaltet und wie mit den personenbezogenen Daten umgegangen werden sollen. Der Gesetzgeber betont, dass von der Möglichkeit der Anonymisierung und Pseudonymisierung Gebrauch zu machen ist.

---

[491] Vgl. Bundesdatenschutzgesetz (BDSG) unter http://bundesrecht.juris.de/bdsg_1990/index.html, Stand: 07.07.2009.

„Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.“

Im BDSG werden die Möglichkeiten der Anonymisierung und Pseudonymisierung wie folgt erläutert:[492]

- Anonymisierung ist in § 3 Abs. (6) BDSG definiert als „*…Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können*.“[493]

- Pseudonymisierung ist in § 3 Abs. (6a) BDSG hingegen definiert als„*…das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.*“[494]

Neben diesen Begriffsbestimmungen enthält Abs. (10) des § 3 BDSG eine Definition bezüglich der „Mobilen personenbezogenen Speicher- und Verarbeitungsmedien“. Dort heißt es:

„*Mobile personenbezogene Speicher- und Verarbeitungsmedien sind Datenträger,*

1. die an den Betroffenen ausgegeben werden,

2. auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können und

3. bei denen der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.“

---

[492] Vgl. mit dem Kapitel Identität und Grade der Anonymität, S. 97ff.

[493] Vgl. BDSG § 3 Weitere Begriffsbestimmungen, http://bundesrecht.juris.de/bdsg_1990/__3.html, Stand: 31.05.2009.

[494] Vgl. Ebenda.

In § 29 BDSG[495] ist das geschäftsmäßige Erheben, Speichern oder Verändern personenbezogener Daten zum Zweck der Übermittlung geregelt.

In § 30 BDSG[496] wird das geschäftsmäßige Erheben und Speichern personenbezogener Daten zum Zweck der Übermittlung in anonymisierter Form geregelt. In diesem Paragraf wird insbesondere die gesonderte Speicherung der Merkmale über die persönlichen und sachlichen Verhältnisse der Personen und deren Zuordnung zu den Personen betont.

„§ 30 Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung in anonymisierter Form

(1) Werden personenbezogene Daten geschäftsmäßig erhoben und gespeichert, um sie in anonymisierter Form zu übermitteln, sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Diese Merkmale dürfen mit den Einzelangaben nur zusammengeführt werden, soweit dies für die Erfüllung des Zwecks der Speicherung oder zu wissenschaftlichen Zwecken erforderlich ist.“

5.3.1.2 Telekommunikationsgesetz

Das Telekommunikationsgesetz (TKG) ist ein Bundesgesetz, das besonders den Wettbewerb im Bereich der Telekommunikation reguliert, sowie die Kontinuität der angebotenen Dienstleistungen sichert.[497] Das TKG besteht aus allgemeinen und speziellen Vorschriften für die Marktteilnehmer, vor allem die Mobilfunknetzbetreiber. Die Inhalte des TKG sind unter anderem die Meldepflicht der Telekommunikationsanbieter bei der Bundesnetzagentur (§ 6 TKG), das unbefugte Abhören von Nachrichten (§ 148 TKG), Vorratsdatenspeicherung von personenbezogenen Daten der Telekommunikationskunden, Datenschutz und Sperrung von Internetseiten.

---

[495] Vgl. BDSG § 29 Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung, http://bundesrecht.juris.de/bdsg_1990/__29.html, Stand: 08.07.2009.

[496] Vgl. BDSG § 30 Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung in anonymisierter Form, http://bundesrecht.juris.de/bdsg_1990/__30.html, Stand: 08.07.2009.

[497] Vgl. Telekommunikationsgesetz, http://bundesrecht.juris.de/tkg_2004/index.html, Stand: 11.07.2009.

In den Paragrafen §§88-115 TKG sind speziellen Vorschriften für das Fernmeldegeheimnis, den Datenschutz und die Öffentliche Sicherheit erfasst. In diesem Gesetz sind neben den allgemeinen Marktregulierungsvorschriften insbesondere die Schutzverpflichtungen der Netzbetreiber sowie deren Informationspflichten gegenüber dem Kunden, also der Schutz personenbezogener Kundendaten geregelt. Es wird jedoch vor allem die Vorratsdatenspeicherung von personenbezogenen Kundendaten kritisiert und diskutiert, da dies nach einem automatisierten Auskunftsverfahren laufen soll.

Wie mit den Verkehrsdaten von Kunden umzugehen ist, ist in § 96 TKG geregelt.[498] Der Gesetzgeber regelt dort die Erhebung, Verwendung und Speicherung von Verkehrsdaten durch Dienstanbieter für bestimmte Zwecke, also unter anderem für die Entgeltermittlung und Entgeltabrechnung, Einzelverbindungsnachweis etc. In § 96 Absatz 3 schreibt der Gesetzgeber „die unverzügliche Anonymisierung der Daten der Teilnehmer“ vor. Die Nutzung der teilnehmerbezogenen Verkehrsdaten ist nur mit der Einwilligung der Teilnehmer zulässig.

Die Verwendung von Standortdaten regelt § 98 TKG.[499] Dieser Paragraf hat eine große Bedeutung, wenn es um die Mobilität bzw. Standortinformationen von Kunden geht. In § 98 Absatz1 wird die Verwendung von Standortdaten für die Bereitstellung von Diensten mit Zusatznutzen und bestimmte Zeit erlaubt, wenn sie anonymisiert wurden oder wenn der Teilnehmer seine Einwilligung erteilt hat.

5.3.1.3 Telemediengesetz

Das Telemediengesetz (TMG)[500], das am 1. März 2007 in Kraft getreten ist, bestimmt die rechtlichen Rahmenbedingungen für Teledienste und Mediendienste in Deutschland. Der Begriff Telemedien ist ein Überbegriff für elektronische Informations- und Kommunikationsdienste. Das TMG ist ein wichtiges Regelwerk für Internetrecht und beinhaltet die Vorschriften, die früher im Teledienstegesetz (TDG), Teledienstedatenschutzgesetz (TDDSG) und Mediendienste-Staatsvertrag (MdStV) verteilt

---

498 Vgl. Telekommunikationsgesetz (TKG), http://bundesrecht.juris.de/tkg_2004/__96.html, Stand: 11. 07.2009.

499 Vgl. Telekommunikationsgesetz (TKG), http://bundesrecht.juris.de/tkg_2004/__98.html, Stand: 11. 07.2009.

500 Vgl. Telemediengesetz (TMG), http://www.gesetze-im-internet.de/tmg/, Stand: 11.07.2009.

waren. Mit dem Inkrafttreten vom TMG sind die zuvor genannten Gesetze außer Kraft getreten.

In § 13 Abschnitt 6 wird dargelegt, dass der Diensteanbieter verpflichtet ist, die Nutzung anonym und unter einem Pseudonym zu gewährleisten, sofern dies technisch möglich und zumutbar ist:

„Der Diensteanbieter hat die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren.“[501]

§ 14 Abschnitt 1 regelt die Erhebung und Verwendung von Bestandsdaten:

„Der Diensteanbieter darf personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind (Bestandsdaten).“[502]

§ 15 Abschnitt 1 regelt die Erhebung und Verwendung von Nutzungsdaten:[503]

„Der Diensteanbieter darf personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (Nutzungsdaten). Nutzungsdaten sind insbesondere

1. Merkmale zur Identifikation des Nutzers,

2. Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und

3. Angaben über die vom Nutzer in Anspruch genommenen Telemedien.

In § 15 Abschnitt 3 wird die Erstellung von Nutzungsprofilen durch die Möglichkeit der Nutzung von Pseudonymen erwähnt.

„Der Diensteanbieter darf für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von

---

501 Vgl. Telemediengesetz (TMG), http://www.gesetze-im-internet.de/tmg/__13.html, Stand: 11.07.2009.

502 Vgl. Telemediengesetz (TMG), http://www.gesetze-im-internet.de/tmg/__14.html, Stand: 11.07.2009.

503 Vgl. Telemediengesetz (TMG), http://www.gesetze-im-internet.de/tmg/__15.html, Stand: 11.07.2009.

Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht. Der Diensteanbieter hat den Nutzer auf sein Widerspruchsrecht im Rahmen der Unterrichtung nach § 13 Abs. 1 hinzuweisen. Diese Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden."

5.3.1.4 Telekommunikations-Überwachungsverordnung

Die Telekommunikations-Überwachungsverordnung (TKÜV), die am 22. Januar 2002 in Kraft getreten ist, regelt die technischen und organisatorischen Voraussetzungen für die Umsetzung von gesetzlich vorgesehenen Maßnahmen zur Überwachung der Telekommunikation.[504] Die TKÜV gilt für die Betreiber der Telekommunikationsanlagen bzw. Anbieter der Telekommunikationsservices. Nach der TKÜV sind die Betreiber der Telekommunikationsanlagen bzw. Anbieter der Telekommunikationsservices verpflichtet, die Kommunikationsdaten (Sprache oder Daten) ihrer Kunden aufzuzeichnen und gegebenenfalls an die Strafverfolgungs- und Sicherheitsbehörden weiterzuleiten. Mit der TKÜV wird die Umsetzung der in § 110 TKG erwähnten Überwachungsmaßnahmen[505] sowie Genehmigungsverfahren nach den § 110a und 110b der Strafprozessordnung[506] festgelegt. Eine Überwachung kann bei Verdacht bestimmter schwerer Straftaten gegen bestimmte Personen bzw. bestimmte Anschlüsse (sog. Individualkontrolle) oder zur Erkennung bestimmter schwerwiegender Gefahren ohne Bezug auf bestimmte Personen (sog. strategische Kontrolle) angeordnet werden. Bei Fällen der Individualkontrolle werden grundsätzlich richterliche Anordnungen benötigt. Bei Fällen der strategischen Kontrolle sind die Anordnungen durch das Bundesministerium des Innern zu erlassen.[507]

Darüber hinaus gibt es Regelungen auf Europäischer Ebene. Ein wichtiges Regelwerk in der Europäischen Union ist die Europäische Datenschutzkonvention, die am 28. Januar 1981 von den damaligen Mitgliedstaaten des Europarats vereinbart wurde

---

504 Vgl. Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation, http://www.gesetze-im-internet.de/tk_v_2005/index.html, Stand: 21.01.2010.

505 Vgl. mit dem § 100 TKG, http://bundesrecht.juris.de/tkg_2004/__110.html, Stand: 21.01.2010. Sowie mit den Erläuterungen im Abschnitt Telekommunikationsgesetz, S. 144.

506 Vgl. mit den § 110a und § 110b der Strafprozessordnung, http://www.gesetze-im-internet.de/stpo/index.html, Stand: 21.01.2010.

507 Vgl. Häufig gestellte Fragen zur TKÜV, http://www.bmwi.de/BMWi/Navigation/technologie-und-innovation,did=6020.html, Stand: 21.01.2010.

und am 1. Oktober 1985 in Kraft trat.[508] Die offizielle Bezeichnung der Europäischen Datenschutzkonvention ist „das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten“.[509] Damit regelt die Europäische Datenschutzkonvention die Rechte und Grundfreiheiten der Vertragsparteien und erwähnt insbesondere die Achtung der grundlegenden Persönlichkeitsrechte beim freien, grenzüberschreitenden Informationsaustausch und Schutz personenbezogener Daten, die automatisiert verarbeitet werden.[510]

5.3.2 Strafrechtliche Aspekte der User-Anonymität

Die Gesetze und Verordnungen zum Datenschutz bzw. zur User-Anonymität bestimmen die Verhältnisse der User und Serviceprovider. Die Anonymität und Pseudonymität bieten Möglichkeiten zum Schutz personenbezogener Daten und der eigenen Identität. Sie eröffnen jedoch auch Personen und Organisationen mit kriminellen Absichten Möglichkeiten zum Missbrauch. Deshalb sollen bei Straftaten und Verdachtsfällen auch strafrechtliche Aspekte der User-Anonymität erläutert werden.

5.3.2.1 Vorratsdatenspeicherung und Überwachung der Netzwerke

Die Gesetze und Verordnungen zwingen die Anbieter der Telekommunikationsanlagen und -dienstleistungen, dass sie die Kommunikationsdaten ihrer User für einen bestimmten Zeitraum speichern und diese Daten für die Strafverfolgung herausgeben sollen. Mit der Vorratsdatenspeicherung werden die Anbieter der Telekommunikationsdienste verpflichtet, alle elektronischen Kommunikationsvorgänge zu speichern, auch wenn kein Anfangsverdacht oder konkrete Hinweise auf Gefahren existieren.

Das EU-Parlament hat am 14.12.2005 eine Richtlinie verabschiedet, mit der die EU alle Anbieter von Telekommunikationsdienstleistungen zum Speichern der

---

[508] Vgl. Mehr Infos über die Unterzeichnung, den Inkrafttreten und die Ratifikationen unter: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=2&DF=10/4/2006&CL=GER, Stand: 12.07.2009.

[509] Vgl. Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, http://conventions.coe.int/Treaty/GER/Treaties/Html/108.htm, Stand: 12.07.2009.

[510] Vgl. Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, http://conventions.coe.int/Treaty/GER/Treaties/Html/108.htm, Stand: 12.07.2009.

Kommunikationsdaten der User für mindestens sechs Monate zwingt. Die Richtlinie soll vor allem die unterschiedlichen nationalen Vorschriften der EU-Mitgliedsstaaten zur Speicherung von Telekommunikationsdaten auf Vorrat vereinheitlicht werden. Durch die Vereinheitlichung soll sichergestellt werden, dass die Telekommunikationsdaten für einen bestimmten Zeitraum für die Zwecke der Ermittlung und Verfolgung von schweren Straftaten gespeichert werden.[511]

Jedoch ist die Richtlinie über Vorratsdatenspeicherung politisch wie rechtlich aufgrund von Grundrechten, dem Fernmeldegeheimnis, dem Recht auf informationelle Selbstbestimmung bedenklich. Einerseits wird die Vorratsdatenspeicherung als ein notwendiges Instrument zur Strafverfolgung der Internetkriminalität, der organisierten Kriminalität und der Terrorismusbekämpfung bezeichnet. Andererseits wird sie heftig als ein direkter Eingriff in die Privatsphäre der Bürger kritisiert.[512]

Im Urteil vom 02.03.2010 wurde die konkrete Gestaltung der Vorratsdatenspeicherung vom Bundesverfassungsgericht als nicht verfassungsmäßig erklärt.[513] Danach verstößt die Vorratsdatenspeicherung gegen die Verfassung. Die Service Provider, die bisher unter den Regeln Daten gespeichert haben, müssen jetzt diese Daten unverzüglich löschen. Gleichzeitig entschieden die Richter eine Vorratsdatenspeicherung im Rahmen der Strafverfolgung und Gefahrenabwehr nicht generell unzulässig. Die Speicherung ist künftig nur unter strengen Anforderungen zulässig.[514]

5.3.2.2 Aufhebung und Aufdeckung der Anonymität des Users

Köpsell und Miosga erläutern in ihrem Beitrag[515] von einem effizienten Verfahren zur datenschutzgerechten Deanonymisierung der Sender und Empfänger für die Strafverfolgung. Danach werden alle Kommunikationsdaten bei den Anonymisierungsdiensten laut einer richterlichen Anordnung protokolliert und schrittweise de-

---

511 Vgl. Die Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten. Ausführliche Informationen finden sich unter http://eurlex.europa.eu/LexUriServ/site/de/oj/2006/l_105/l_10520060413de00540063.pdf, Stand: 14.07.2009.

512 Vgl. Hoeren (2009), S. 494ff. Diese Kritik wurde im Urteil zur Vorratsdatenspeicherung vom 02.03.2010 des Bundesverfassungsgerichts bekräftigt. Vgl. Müller (2010a).

513 Vgl. Müller (2010a); Müller (2010).

514 Vgl. Müller (2010a); BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. (1 - 345), http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html, Stand: 03 03.2010.

515 Vgl. Köpsell/Miosga (2005), S. 403.

anonymisiert. Die Deanonymisierung der Kommunikationsbeziehungen enthüllt jedoch nicht die Identität einer Person, sondern es werden Indizien (IP-Adressen, Metadaten etc.) gesammelt, die Rückschlüsse auf die Identität des Senders und des Empfängers erlauben.[516]

Die Strafverfolgung fordert, dass im Falle eines Missbrauchs der Anonymität eine nachträgliche Aufdeckung einer Verbindung möglich ist.[517] Deshalb werden die Anonymisierungsdienste aufgrund der Vorratsdatenspeicherung verpflichtet, die Kommunikationsdaten auf Vorrat zu speichern, die dann eine rückwirkende Aufdeckung der Anonymität erleichtern können.[518] Für eine Überwachung zukünftiger Verbindungen muss die Ein-Ausgabe-Zuordnung der Nachrichten sofort online mitprotokolliert und die Verbindungen markiert werden. Somit können die Nachrichten unter Beteiligung aller Anonymisierungsdienstanbieter deanonymisiert werden. Die Markierung der Verbindungen kann nur von beteiligten Anonymisierungsdienstanbietern erkannt werden.[519] Die Anonymisierungsdienstanbieter protokollieren alle Zugriffe auf eine bestimmte Webseite. Somit ist die Anonymität nicht mehr gewährleistet, da eine Überwachung der Anonymisierungsdienste stattfindet.[520]

5.3.2.3 Herausgabe der Bestandsdaten

Die Gesetze und Verordnungen erfordern bei bestimmten Straftaten oder Verdachtsfällen die Herausgabe der Bestandsdaten, also personenbezogene Daten. In § 14 Absatz 2 TMG wird die Erteilung der Auskunft über die Bestandsdaten durch Service Provider geregelt. Danach dürfen bzw. müssen Service Provider Auskunft über Bestandsdaten der User (personenbezogene Daten) nach § 14 Absatz 2 TMG erteilen, soweit dies für die Zwecke der Strafverfolgung etc. erforderlich ist. Dort heißt es:

---

516 Vgl. Ebenda.

517 Die Implementierung dieser Forderung für die Strafverfolgung ist umstritten. Vgl. JAP und Strafverfolgung - Rückwirkende Aufdeckung von Verbindungen durch die Mix-Kaskaden, Ausführliche Informationen finden sich unter http://anon.inf.tu-dresden.de/strafverfolgung/index_de.html, Stand: 14.07.2009.

518 Vgl. JAP und Strafverfolgung - Rückwirkende Aufdeckung von Verbindungen durch die Mix-Kaskaden, http://anon.inf.tu-dresden.de/strafverfolgung/index_de.html, Stand: 14.07.2009.

519 Vgl. JAP und Strafverfolgung - Überwachung zukünftiger Verbindungen durch die Mix-Kaskaden, http://anon.inf.tu-dresden.de/strafverfolgung/index_de.html, Stand: 14.07.2009.

520 Vgl. JAP und Strafverfolgung - Erfahrungen des Projektes "AN.ON" im Bereich Strafverfolgung, http://anon.inf.tu-dresden.de/strafverfolgung/index_de.html, Stand: 14.07.2009.

§ 14 Bestandsdaten Absatz (2):

„Auf Anordnung der zuständigen Stellen darf der Diensteanbieter im Einzelfall Auskunft über Bestandsdaten erteilen, soweit dies für Zwecke der Strafverfolgung, zur Gefahrenabwehr durch die Polizeibehörden der Länder, zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes oder des militärischen Abschirmdienstes oder des Bundeskriminalamtes im Rahmen seiner Aufgabe zur Abwehr von Gefahren des internationalen Terrorismus oder zur Durchsetzung der Rechte am geistigen Eigentum erforderlich ist.“

Damit stellt § 14 Absatz 2 klar, dass ein Anspruch auf die Auskunftserteilung für die Strafverfolgung besteht und dieser nicht automatisch aufgrund des Datenschutzes gesperrt ist. Dieser Anspruch auf die Auskunft ist auch in der Strafprozessordnung niedergelegt.

5.3.2.4 Herausgabe der Verkehrsdaten

Für die Verfolgung und Aufklärung der Straftaten mittels Telekommunikation besteht ein Anspruch auf die Herausgabe der Verkehrsdaten. So kann ein Richter oder Staatsanwalt die Herausgabe von Verkehrsdaten nach § 100g StPO und § 113a TKG anordnen, die von Telekommunikationsdienstanbieter auf Vorrat gespeichert sind.

In § 113a TKG regelt, welche Daten für speicherungspflichtig sind. Danach werden Telekommunikationsdienstanbieter verpflichtet, bestimmte Verkehrs- und Standortdaten, die bei der Nutzung von Telefon, Mobiltelefon, E-Mail und Internet erzeugt bzw. verarbeitet werden, für einen Zeitraum von 6 Monaten zu speichern.

In § 113b TKG wird die Verwendung der nach § 113a gespeicherten Daten geregelt:

„Der nach § 113a Verpflichtete darf die allein auf Grund der Speicherungsverpflichtung nach § 113a gespeicherten Daten

1. zur Verfolgung von Straftaten,

2. zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit oder

3. zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes und des militärischen Ab-

schirmdienstes an die zuständigen Stellen auf deren Verlangen übermitteln, soweit dies in den jeweiligen gesetzlichen Bestimmungen unter Bezugnahme auf § 113a vorgesehen und die Übermittlung im Einzelfall angeordnet ist; für andere Zwecke mit Ausnahme einer Auskunftserteilung nach § 113 darf er die Daten nicht verwenden. § 113 Abs. 1 Satz 4 gilt entsprechend."

Allerdings ist die Vorratsdatenspeicherung und die Herausgabe der Verkehrsdaten nach § 113b aufgrund des Beschlusses (1 BvR 256/08 vom 28.10.2008)[521] des 1. Senat des Bundesverfassungsgerichts eingeschränkt. Aufgrund dieses Beschlusses dürfen Strafverfolgungsbehörden bis zum Ablauf von sechs Monaten nur unter eingeschränkten Bedingungen die gespeicherten Daten verwenden.[522]

Zusammenfassend kann festgehalten werden, dass die regulatorischen Rahmenbedingungen zusammen mit den EU-Datenschutzrichtlinien eine breite Basis für die rechtliche Gestaltung der anonymen Mobile Payment Systeme bieten. Allerdings wird das letzte Urteil zur Vorratsdatenspeicherung neue Wirkungen auf die Gesetzgebung und damit auf die Gestaltung regulatorischer Rahmenbedingungen haben, die den Datenschutz und Umgang mit den Bestands-, Verbindungs- und Standortdaten bestimmen. So wird der Gesetzgeber die vorhandenen relevanten Gesetze bzw. Paragraphen in BDSG, TKG, TMG sowie TKÜV in nächster Zeit modifizieren und verfassungsmäßig gestalten müssen.[523]

---

[521] Vgl. BVerfG, 1 BvR 256/08 vom 28.10.2008, Absatz-Nr. (1 - 118). Ausführliche Informationen finden sich unter http://www.bverfg.de/entscheidungen/rs20081028_1bvr025608.html, Stand: 14.07.
2009.

[522] Vgl. mit den Erläuterungen im Abschnitt 5.3.2.1 Vorratsdatenspeicherung und Überwachung der Netzwerke, S. 148, insb. mit den Erläuterungen des Urteils zur Vorratsdatenspeicherung.

[523] Vgl. o. V. (2010d); Müller (2010a); Müller (2010b) sowie mit den Erläuterungen über das neue Urteil zur Vorratsdatenspeicherung vom 02.03.2010 im Abschnitt 5.3.2.1 Vorratsdatenspeicherung und Überwachung der Netzwerke, S. 148.

6 User-Anonymität in Mobile Payment Systemen

In diesem Kapitel wird zunächst eine Analyse der Mobile Payment Wertschöpfungskette sowie eine Analyse eines allgemeinen, gegenwärtig in der Praxis geläufigen Mobile Payment Prozesses durchgeführt. Anschließend wird der allgemeine Mobile Payment Prozess hinsichtlich der User-Anonymität bewertet. Dabei wird gezeigt, in welchen Prozessschritten es an User-Anonymität mangelt bzw. anonymisiert werden sollte. Im nächsten Abschnitt wird ein neues organisatorisches Konzept zur Gestaltung der User-Anonymität in Mobile Payment Systemen dargestellt und wird in einem neuen Referenzprozessmodell anhand eines Praxisbeispiels erläutert. Aufgrund der komplexen Prozessabläufe wird dieses Modell auf einer hohen Abstraktionsebene (High-Level) dargestellt. Dabei werden die einzelnen Mobile Payment Prozesse im Referenzprozessmodell detailliert beschrieben. Im letzten Abschnitt wird die User-Anonymität gegenüber den Marktteilnehmern im Referenzprozessmodell bewertet, um zu zeigen, welche Marktteilnehmer welche Daten erhalten und ob bzw. wie anonym der mobile User ist und wie er seine Identität in Mobile Payment Systemen selber bestimmen kann.

6.1 Analyse der Mobile Payment Wertschöpfungskette

Die Mobile Payment Wertschöpfungskette besteht potentiell aus den in der Abbildung 27, S. 154 dargestellten Teilnehmern. Diese übernehmen im Mobile Payment System verschiedene Rollen und vertreten verschiedene Interessen.[524] Aufgrund der einfachen Veranschaulichung der Mobile Payment Wertschöpfungskette werden hier nicht alle Marktteilnehmer, sondern nur die Hauptteilnehmer im Mobile Payment System dargestellt.[525]

Der Webshopbetreiber oder Mobile Content Provider (MCP) sowie der mobile User befinden sich am Anfang bzw. Ende der Wertschöpfungskette. Der Webshopbetreiber oder Content Provider bietet verschiedene Produkte und Services in mobiler Umgebung. Der mobile User kauft bzw. bezahlt diese Produkte oder Services. Zwischen beiden Teilnehmern, dem mobilen User und dem MCP, befinden

---

[524] Dies wird bereits im Abschnitt 3.1 Teilnehmer und Rollen im Mobile Payment Ökosystem, S. 55 erläutert.

[525] Ausführliche Informationen über alle Marktteilnehmer finden sich im Abschnitt 3.1 Teilnehmer und Rollen im Mobile Payment Ökosystem, S. 55.

sich andere Marktteilnehmer entlang der Wertschöpfungskette. Die Banken oder Kreditkartengesellschaften führen den Zahlungsverkehr bzw. die Zahlungsbegleichung aus, welche in der Regel im Hintergrund ablaufen.

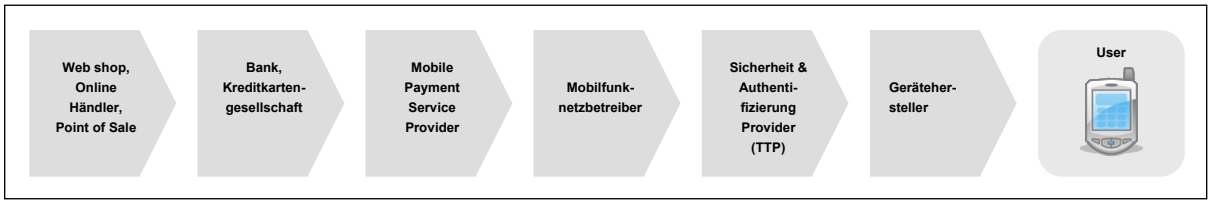

Abbildung 27: Mobile Payment Wertschöpfungskette[526]

Die Mobile Payment Service Provider (MPSP) stellen mobile Zahlungsdienste bereit bzw. führen diese zusammen mit den Banken und Kreditgesellschaften aus. Die Mobilfunknetzbetreiber stellen die gesamte Telekommunikationstechnik und den Datenübertragungservice zur Verfügung. Die Mobilfunknetzbetreiber nutzen ihre Billing-Infrastruktur auch für die Mobile Payments. Für die Sicherheit und Authentifizierung der mobilen User sorgen die Trusted Third Parties (Vertrauensinstanzen). Die Gerätehersteller entwickeln bzw. vertreiben innovative und markgerechte Mobilfunkgeräte, die sich für die Anwendungen in den Bereichen Mobile Commerce und Mobile Payment eignen.

Die einzelnen Prozessabläufe in der Mobile Payment Wertschöpfungskette werden im nächsten Abschnitt in einem allgemeinen, in der Praxis geläufigen Mobile Payment Prozess detailliert ausgeführt.

6.2 Analyse eines allgemeinen Mobile Payment Prozesses

Die Prozessabläufe von Mobile Payment Systemen sind in der Praxis je nach Anbieter dieser Systeme unterschiedlich organisiert. Allgemein jedoch werden die einzelnen Prozesse von Mobile Payment Systemen, wie in der Abbildung 28, S. 155 dargestellt, organisiert. Dieser allgemeine Mobile Payment Prozess kann wie folgt erklärt werden:

Der mobile User befindet sich am Anfang der Wertschöpfungskette, der mit einer Serviceanfrage einen Kaufprozess und damit einen Zahlungsprozess initiiert. Dem User gegenüber stehen MCP und MPSP, die die Serviceanfrage des Users an-

526 In Anlehnung an Dahlberg et al. (2006), S. 3; Sekino/Kwon/Bong (2007), S. 3ff.

nehmen bzw. diese bearbeiten und das gewünschte Produkt oder den Service an den User senden. Neben diesen Akteuren spielt die TTP im Prozess eine ganz wichtige Rolle, die u. a. für die Authentifizierung des Users verantwortlich ist. Nach der Authentifizierung des Users wird der Einkauf bzw. die Serviceanfrage autorisiert. Jetzt kann das Produkt bzw. der Service geliefert werden. Nach der Lieferung erfolgt in der Regel das Billing vom Payment Service Provider. Am Ende des Prozesses erfolgt letztlich die Bezahlung („Payment“) durch den mobilen User.

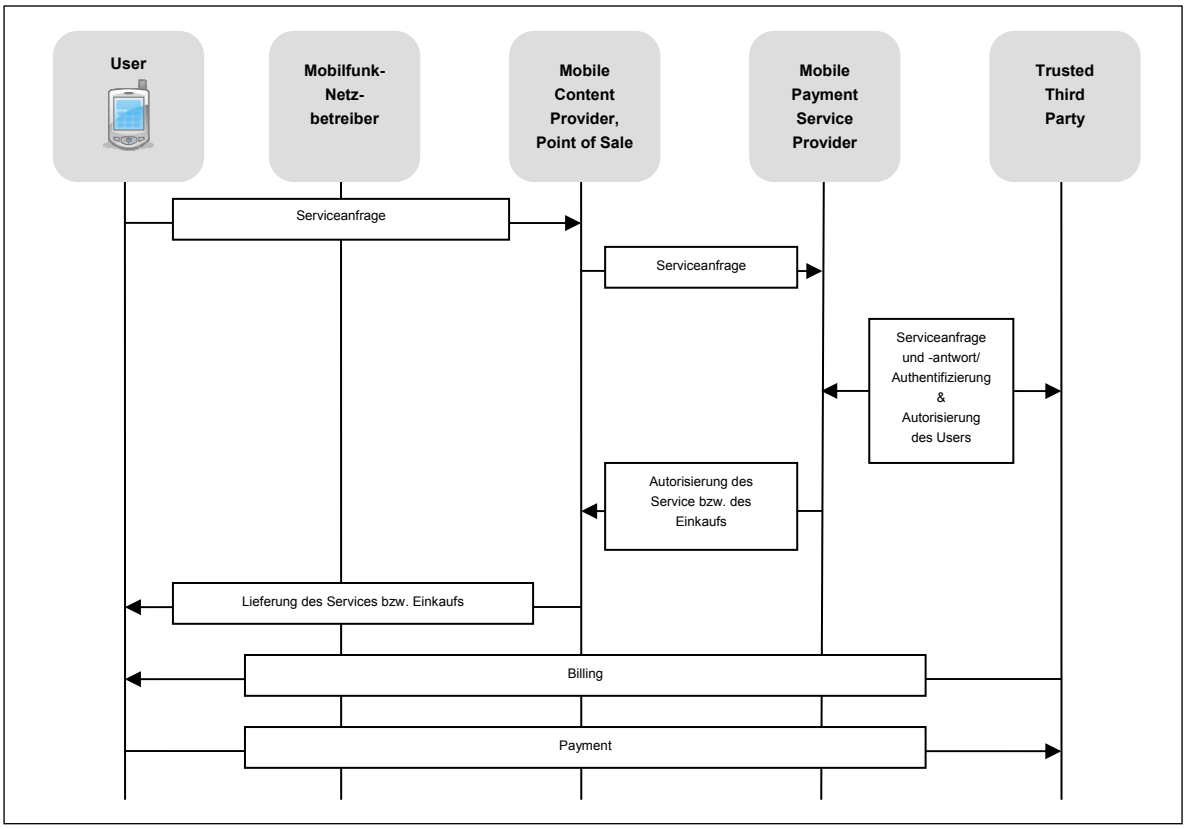

Abbildung 28: Allgemeiner Mobile Payment Prozess[527]

Der allgemeine Mobile Payment Prozess kann in einer Reihe von Prozessschritten beschrieben werden, die vom Electronic Payment Prozess im Internet übernommen wurden. Ein Electronic Payment Prozess im Internet besteht in der Regel aus vier Phasen:[528]

1. Phase: die Setup und Konfiguration oder Registrierung

2. Phase: die Initialisierung des Payments

---

527 In Anlehnung an Hu/Lee/Kou (2005), S. 194.

528 Vgl. Lee/Hu/Kou (2007), S. 301ff. Jain/Seri/Srinivasan (2008), S.16ff.

3. Phase: Authentifizierung des Users

4. Phase: die Ausführung und Fertigstellung des Payments

In einem allgemeinen Mobile Payment Prozess zeigen sich ähnliche Abläufe. Die Prozessabläufe unterscheiden sich jedoch in den jeweiligen Mobile Payment Anwendungen. Daher gibt es in der Praxis verschiedene Ausprägungen für den Mobile Payment Prozess. Für die Analyse wird hier ein allgemeiner Mobile Payment Prozess dargestellt, der in drei Phasen wie folgt erklärt werden kann: [529]

1. Phase: Registrierung

2. Phase: Transaktion

    2.1. Serviceanfrage

    2.2. Initialisierung des Payments

    2.3. Authentifizierung des mobilen Users

    2.4. Ausführung bzw. Lieferung des Services

3. Phase: Fertigstellung des Payments

wobei sich die 2. Phase Transaktion nochmals in vier Unterphasen unterteilt. Die Phasen und Unterphasen können wie folgt beschrieben werden:

1. Phase Registrierung: Der mobile User registriert sich einmalig bei einem Mobile Payment Service Provider (MPSP) und eröffnet damit ein Konto zur Nutzung des Payment Services mit einer bestimmten Payment-Methode. Bei der Erstregistrierung handelt es um eine einmalige Transaktion, die nicht bei jedem weiteren Payment wiederholt werden muss. Der mobile User nutzt eine dafür bestimmte PIN für die Identifizierung und Authentifizierung. Damit wird der Zugang des Users zu den Mobile Payment Services sichergestellt. Der User erhält dadurch detaillierte Serviceinformationen wie Content- und Zahlungsart sowie Zahlungsbestätigung.

2. Phase Transaktion: In dieser Phase wird eine mobile Zahlungstransaktion in vier Schritten durchgeführt:

[529] Vgl. Hu/Lee/Kou (2005), S. 194ff.

2.1. Serviceanfrage: Der mobile User möchte einen Content durch die Nutzung des Mobilfunkgerätes herunterladen, indem er in der Regel eine SMS sendet oder wenn er ein spezielles Java-Programm auf seinem Mobilfunkgerät installiert hat, automatisch per Knopfdruck einen beliebigen Content herunterlädt.

2.2. Initialisierung des Payments: Content Provider leitet diese Serviceanfrage des mobilen Users an den MPSP weiter und initiiert das Mobile Payment. Bevor ein Payment initialisiert wird, muss der mobile User bestätigen, dass er für den Service zu zahlen bereit ist. Der MPSP sendet eine Anfrage für die Zahlungsautorisierung an den User in Form einer AGB zwischen User und Content Provider. Nach der Bestätigung der AGB wird das Payment initiiert. Der User muss außerdem den MPSP autorisieren und schickt seine PIN an den MPSP. Die Authentifizierung und Autorisierung erfolgen gleichzeitig mit der PIN-Eingabe.[530]

2.3. Authentifizierung des mobilen Users: Der MPSP überprüft dann bei der TTP die Authentifizierung und Autorisierung des mobilen Users. Der MPSP teilt dem Content Provider das Ergebnis der Authentifizierung des Users mit. Wenn das Ergebnis der Authentifizierung des Users positiv ist, sendet der MPSP dem Content Provider eine Sitzungs-ID[531], die auf die Initialisierung des Payments hinweist.[532]

2.4. Ausführung bzw. Lieferung des Services: Der MPSP informiert dann den Content Provider über die Authentifizierung und Autorisierung des mobilen Users. Nachdem der mobile User erfolgreich authentifiziert und autorisiert wird, kann der Content Provider den gekauften Content an den mobilen User liefern. Dafür

---

[530] Vgl. Lee/Hu/Kou (2007), S. 302.

[531] Eine Sitzungs-ID (engl. Session-ID) ist eine Nummer, die der Server einer Website einmalig an einen spezifischen User für die Dauer seines Besuchs (Session) vergibt. Die Sitzungs-ID kann in einem Cookie, in einem Formular oder dem URL (Uniform Resource Locator) aufbewahrt werden. Einige Webserver erzeugen Sitzungs-IDs einfach durch die Erweiterung von statischen Nummern. Die meisten Server jedoch verwenden Algorithmen mit komplexeren Methoden, wie z.B. die Berücksichtigung von Datum und Zeit des Besuchs zusammen mit anderen, vom Server-Administrator definierten Variablen. Jedes Mal, wenn ein Internet-User eine spezifische Website besucht, wird eine neue Sitzungs-ID vergeben. Einen Browser zu schließen, ihn wieder zu öffnen und die Site noch einmal zu besuchen, erzeugt eine neue Session-ID. Manchmal jedoch wird dieselbe Session-ID beibehalten, solange der Browser geöffnet ist, sogar dann, wenn der User die besagte Site verlässt und zurückkehrt. In einigen Fällen beendet der Webserver die Session und vergibt nach einigen Minuten der Inaktivität eine neue Session-ID. Vgl. http://www.searchsecurity.de/glossar/Session-ID/articles/182109/, Stand: 06.03.2010.

[532] Vgl. Lee/Hu/Kou (2007), S. 302.

autorisiert er den Service oder Einkauf. Dann erfolgt die Lieferung des Services oder Einkaufs.

3. Phase Fertigstellung des Payments: In dieser Phase wird der Content durch die jeweilige Mobile Payment Methode bezahlt. Es gibt drei Methoden: Prepaid, Paynow, Postpaid.[533] Bei der Paynow-Methode wird die Zahlungstransaktion beispielsweise durch ein bankkontenbasiertes System in Echtzeit durchgeführt, z. B. Sofortüberweisung von Payment Networks oder Kreditkartenbelastung. Bei der Prepaid-Methode kann der mobile User die Zahlung im Voraus mit sog. Smartkarten oder elektronischen Geldbörsen durchführen. Bei der Postpaid Methode sendet der MPSP die Rechnung an die TTP, die diese Rechnung dann zum mobilen User sendet. Danach schickt sie das Geld an den MPSP.

Dieser Mobile Payment Prozess mit drei Phasen ist systemübergreifend sehr allgemein beschrieben. Daher können die Operationsphasen je nach Mobile Payment Methode variieren. Es gibt Standardisierungsbemühungen seitens der Mobile Payment Initiativen.[534] So arbeitet Mobile Payment Forum an einer Standardisierung der Operationsphasen im Mobile Payment Lebenszyklus, die mit den folgenden Stufen durchgeführt wird: [535]

1. Phase Setup und Konfiguration: Der mobile User konfiguriert sein Mobilfunkgerät für die Nutzung der Payment-Funktion in der Mobile Payment Umgebung. Die Setup und Konfiguration kann über das Mobilfunknetzwerk, Internet oder physisch erfolgen.

2. Phase Payment Initialisierung: In dieser Phase werden die Zahlungsdaten einer Transaktion über ein Netzwerk an den Händler übermittelt, damit er seine Leistungen geltend machen kann.

3. Phase Authentifizierung: Die Authentifizierung des Users ist ein essentieller Teil jeder Zahlungstransaktion. Die Mobile Payment Forum erwägt eine bidirektionale Datentransfer-Authentifizierung[536] und SAT (SIM-Alliance/Application Toolkit)[537]

---

533 Vgl. mit den Erläuterungen im Abschnitt 2.4 Mobile Payment Typen, S. 23.

534 Vgl. mit den Erläuterungen im Abschnitt 2.8 Mobile Payment Initiativen, S. 49.

535 Vgl. Lee/Hu/Kou (2007), S. 303ff. sowie mit dem Abschnitt 2.8.3 Mobile Payment Forum, S. 52.

536 Bei der bidirektionalen Datentransfer-Authentifizierung müssen beide Parteien der jeweils anderen ihre Identität nachweisen, wann immer ein Datentransfer zwischen Client und Server stattfindet. Dies geschieht auf der Basis der asymmetrischen Verschlüsselung. Vgl. Fröming/Gronau/Aethner (2007), S. 111; Vgl. dazu auch mit den Erläuterungen über die Verschlüsselungstechniken im Ab-

Fortsetzung auf der nächsten Seite

Authentifizierung-Anwendungen. Die Standardisierung der SAT-Authentifizierung umfasst eine Reihe von Mindestanforderungen für die Authentifizierung; Damit können die Transaktionskosten der Verbindungen erheblich gesenkt werden.

4. Payment Fertigstellung: Dieser Prozess findet statt, nachdem der User authentifiziert und die Zahlungstransaktion autorisiert ist. Dies umfasst in einer POS-Transaktion einen Druckvorgang für eine Quittung für den User, um zu bestätigen, dass das Geld übertragen wurde. In der mobilen Umgebung wird eine digitale Rechnung erstellt.

In den dargestellten Mobile Payment Prozessen stehen vorwiegend die technische Machbarkeit, die Kosten und die Sicherheit der Transaktionen im Vordergrund. Deshalb wird das Augenmerk nicht oder nur unzureichend auf die Anonymität der User gesetzt. Die ausführliche Bewertung der User-Anonymität in den dargestellten Mobile Payment Systemen erfolgt im folgenden Abschnitt.

6.3 Bewertung des allgemeinen Mobile Payment Prozesses hinsichtlich der User-Anonymität

Die vorgestellten Modelle der Mobile Payment Systeme erfordern eine Registrierung der mobilen User. Die Registrierung wird mit der Angabe der personenbezogenen Daten vom mobilen User beim Händler und MPSP durchgeführt. Dies erfolgt schon in der ersten Phase der Kauf- bzw. Zahlungstransaktion. Alle Prozessbeteiligten erhalten diese personenbezogenen Daten ganz oder teilweise. Zwar verpflichten sich die Prozessbeteiligten gesetzlich, dass diese Daten vertraulich behandelt werden, jedoch ist ein berechtigter Zweifel an diesem Prozess der vertraulichen Behandlung angebracht.

Damit der Kauf- bzw. Zahlungsprozess ablaufen kann, muss sich der User authentifizieren. Das heißt, der User muss sich gegenüber seinen Geschäftspartnern wie Händlern identifizieren lassen. Für die Autorisierung der Käufe muss er seine Identi-

---

schnitt 3.1.7 Trusted Third Party, S. 60 sowie im Abschnitt 7.4.3 Berücksichtigung digitaler Verschlüsselungstechniken und Signaturen, S. 197.

537 Der SAT-Standard basiert auf die GSM-Technologie und ermöglicht es der SIM-Karte auf dem Mobilfunkgerät, einen interaktiven Austausch zwischen der Netzwerkanwendung und dem User zu initiieren. Der SAT-Standard ermöglicht auch eine höhere Sicherheit durch Identitätsprüfung und Verschlüsselung für die Transaktionen im E-Commerce. Vgl. http://www.cellular.co.za/sim_toolkit.htm, Stand: 06.03.2010.

tät ebenso offenbaren. Auch in dieser Phase hinterlässt der User Datenspuren beispielsweise, welches Produkt oder welchen Service, er wo und in welcher Menge anfragt bzw. kauft.

Wie im vorigen Abschnitt in den Mobile Payment Prozessen dargestellt, hinterlässt der User in den Phasen der Kauf- und Zahlungsprozesse seine Transaktions- und personenbezogenen Daten. Daher kennen die Prozessbeteiligten die wahre Identität des Users. Die Schwachstellen der vorgestellten Mobile Payment Prozesse finden sich hinsichtlich der User-Anonymität in allen Phasen. Diese werden im nächsten Abschnitt sichtbar gemacht.

Im Folgenden wird gezeigt, wer welche Daten und Informationen benötigt, damit die Geschäftsprozesse gestaltet werden, in welchen Phasen des Mobile Payment Prozesses eine Anonymisierung des Users benötigt wird und welche Maßnahmen und Regelungen für diesen Zweck erforderlich sind. Dafür wird ein neues Referenzprozessmodell eingeführt. Hierbei wird dargestellt, was der User benötigt, damit er mobil bezahlen kann und wie die Maßnahmen und Regelungen zur Gestaltung der User-Anonymität in diesem Referenzprozessmodell funktionieren. Dabei wird auf die folgenden Fragen eingegangen: Wie kann der User anonym bezahlen? Muss er alle personenbezogenen Daten an die anderen Teilnehmer senden? Was sind seine Interessen im datenschutzrelevanten Sinne?

6.4 Referenzprozessmodell zur Gestaltung der User-Anonymität in Mobile Payment Systemen

In diesem Kapitel wird ein neuer und anonymer Mobile Payment Prozess, in dem eine User-Anonymität ermöglicht wird, in einem Referenzprozessmodell anhand eines Praxisbeispiels dargestellt. Für diesen Zweck werden zunächst die einzelnen Mobile Payment Prozessabläufe im Referenzprozessmodell beschrieben. Als Praxisbeispiel wurde Mobile Content Download gewählt, da dieser eine der erfolgreichsten Mobile Commerce bzw. Mobile Payment Anwendungen ist. Danach wird die User-Anonymität gegenüber den Prozessbeteiligten im Referenzprozessmodell bewertet. Nach der Bewertung der User-Anonymität sollen Wege gezeigt werden, wie das Referenzprozessmodell in die Praxis umgesetzt werden kann. Dabei soll erörtert werden, welche Anforderungen und Rahmenbedingungen bei der Realisierung des Referenzprozessmodells berücksichtigt werden müssen. Anschließend soll auf die möglichen Risiken, Fragen und Probleme sowie deren Lösungsmöglichkeiten hingewiesen werden.

6.4.1 Beschreibung des anonymen Mobile Payment Prozesses

Ein für den User anonymer Mobile Payment Prozess kann in einem Referenzprozessmodell dargestellt werden, in dem ein unabhängiger Anonymitätsservice zum Einsatz kommt. Der Anonymitätsservice ist ein unabhängiger Intermediär, der für die Anonymität des mobilen Users sorgt. Mit dem Service eines solchen Intermediären soll der mobile User in der Lage sein, seine Identität gegenüber den Händlern und anderen am Prozess beteiligten Parteien selbst steuern zu können.[538] Das heißt, der mobile User soll in der Lage sein, selber zu entscheiden, ob er anonym mit seinem Mobilfunkgerät bezahlen möchte oder nicht, wobei diese Anonymität des Users verschiedene Grade haben kann.[539] Danach kann der mobile User mit seiner Entscheidung nicht anonym, anonym oder pseudonym bezahlen. Nach dem hier vorgestellten Lösungsansatz muss sich der mobile User beim MCP weder in der Registrierungs-, noch in der Transaktions-, noch in der Payment-Ausgleichsphase registrieren. Der Mobile Payment Prozess verläuft für den mobilen User vollständig anonym.

Damit ein solcher Lösungsansatz beschrieben werden kann, soll die Anonymität des Users anhand eines Szenarios vom Mobile Content Download veranschaulicht werden:[540] Ein mobiler User möchte bei einem MCP einen Content wie z. B. Musikstücke oder Videos herunterladen oder Mobile Content Service wie z. B. News nutzen. Er startet mit einer anonymen Serviceanfrage und dann bekommt er seinen Service und Rechnung bzw. Zahlungsforderung. Danach werden in einem anonymen Mobile Payment Prozess folgende Prozessschritte durchgeführt:

1. Schritt: Anonyme Serviceanfrage und Schlüsselübertragung[541]
2. Schritt: Authentifizierung des Users
3. Schritt: Autorisierung und Lieferung des Service
4. Schritt: Billing
5. Schritt: Payment

---

538 Vgl. Heuer/Ulmer (2006), S. 5ff.

539 Die Stufen der Anonymität werden im Abschnitt 4.4 Identität und Grade der Anonymität, S. 98 ausführlich behandelt.

540 Vgl. mit den Erläuterungen im Abschnitt Mobile Content Download, S. 41.

541 Gemeint ist hier der öffentliche Schlüssel im asymmetrischen Verschlüsselungsverfahren. Vgl. mit den Erläuterungen im Abschnitt 3.1.7 Trusted Third Party, S. 60 sowie im Abschnitt 7.4.3 Berücksichtigung digitaler Verschlüsselungstechniken und Signaturen, S. 197.

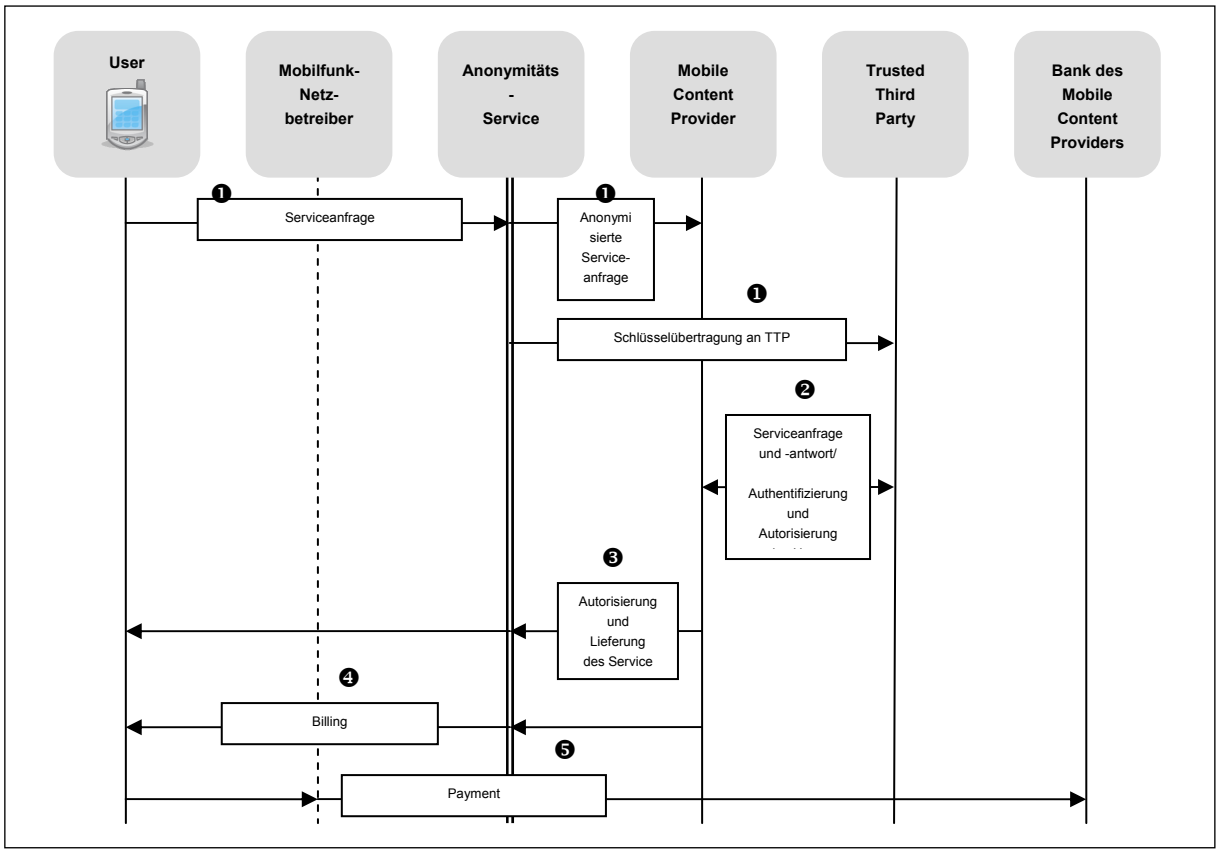

Abbildung 29: Anonymer Mobile Content Download und Mobile Payment Prozess

In der Abbildung 29 werden die Schritte des einem anonymen Mobile Payment Prozesses veranschaulicht, die wie folgt beschrieben werden:

1. Schritt: Anonyme Serviceanfrage und Schlüsselübertragung

Der mobile User fragt beim MCP einen Mobile Content an. Bei dieser Anfrage schaltet er, wenn er gegenüber dem MCP anonym bleiben möchte, auf dem WAP-Browser-fähigen Mobilfunkgerät automatisch oder manuell über eine Applikation (wie z. B. JAP-Software) einen Anonymitätsservice ein.[542] Der User kann mit einer solchen Applikation kann festlegen, welche Daten er an den MCP übertragen soll. Hierbei werden die Mobilfunknummer, mobile IP-Adresse, SIM-Kartennummer und IMEI-Nummer des Mobilfunkgerätes vom User verborgen bzw. nicht übertragen. Die Anfrage geht über den Anonymitätsservice in anonymisierter Form automatisch an den MCP. Bei der Anfrage kann der MCP die personenbezogenen Daten (Mobilfunknummer, SIM-Kartennummer, mobile IP-Adresse und IMEI-Nummer) des mobilen

[542] Vgl. Pfitzmann (2006), S. 21ff. sowie mit den Erläuterungen über die JAP-Software im Abschnitt 5.2.4.4 Mixe und deren Anwendung in der Praxis, S. 133ff.

Users nicht sehen. Stattdessen sieht der MCP nur die anonymisierte Form der mobilen IP-Adresse oder ein Pseudonym des mobilen Users.[543] Der User kann selber entscheiden, welche Anonymitätsgrade er wählen möchte. Beispielsweise sieht der MCP bei einer Anwendung des anonymen Proxy nur die anonymisierte Form der mobilen Adresse.[544] Mit Hilfe des Pseudonym, den der User vom Anonymitätsservice bekommt, kann der MCP seine Leistungen gegenüber dem anonymen User geltend machen. Gleichzeitig werden mit der Serviceanfrage des Users die Userdaten verschlüsselt an die TTP übertragen. Der öffentliche Schlüssel des Users wird bei der TTP für die Authentifizierung und Autorisierung des Users hinterlegt.[545]

2. Schritt: Authentifizierung des Users

Für die Anonymität des Users sorgt der Anonymitätsservice, der eine Kopie der Anfrage mit den verschlüsselten Userdaten an die TTP sendet. Die TTP führt dann die Authentifizierung und Autorisierung des Users durch. Wenn der MCP die anonymisierte Serviceanfrage erhält, dann fordert er bei der TTP die Prüfung der Authentifizierung und Autorisierung des Users. Die TTP antwortet dann auf die Anfrage und teilt dem MCP das Ergebnis der Authentifizierungs- bzw. Autorisierungsprüfung mit. Außerdem sorgt der Anonymitätsservice zusammen mit der TTP für eine eventuelle Rückverfolgung der anonymen Zahlungstransaktionen, wenn es zum Missbrauch bzw. zur Strafverfolgung kommt. Die Rückverfolgbarkeit der anonymen Transaktionen sowie des anonymen Users wird im Folgenden nochmals ausführlicher behandelt.[546]

3. Schritt: Autorisierung und Lieferung des Service

Wenn die Authentifizierung und Autorisierung des Users (positiv) erfolgt, dann autorisiert der MCP die anonyme Serviceanfrage des Users. Dann liefert er den Service an den mobilen User, z. B. an sein Pseudonym.

---

543 Vgl. mit dem Abschnitt 5.2.4 Anonymitätskonzepte, S. 124ff.

544 Vgl. mit dem Abschnitt 5.2.4.1 Proxies und deren Anwendung in der Praxis, S. 125 und dem Abschnitt 5.2.4.3 mCrowds und deren Anwendung in der Praxis, S. 132.

545 Vgl. Heuer/Ulmer (2006), S. 7ff.

546 Vgl. Heuer/Ulmer (2006), S. 7ff. Die Rückverfolgbarkeit der anonymen Transaktionen sowie des anonymen Users wird im Abschnitt 5.3.2.2 Aufhebung und Aufdeckung der Anonymität des Users, S. 149 und im Abschnitt 7.3.3 Einrichtung eines Anonymitätsservices, S. 182 sowie im Abschnitt 7.5.2 Berücksichtigung strafrechtlicher Aspekte, S. 201 detailliert ausgeführt.

4. Schritt: Billing

Nach der Lieferung des Service schickt der MCP eine Rechnung (Billing) mit der Zahlungsforderung an den Mobilfunknetzbetreiber. Im Billing sind das Pseudonym des Users und der gelieferte Service und Betrag angegeben. Das Billing geht über den Anonymitätsservice zum Mobilfunknetzbetreiber. Der Mobilfunknetzbetreiber stellt die Leistungen von MCP in Rechnung und sendet diese am Monatsende an den Mobilfunkuser.

5. Schritt: Payment

Nach Erhalt der Mobilfunkrechnung kann das Payment auf verschiedenste Weise geschehen. Die Mobilfunkrechnung kann mit Lastschriftverfahren beglichen werden. Der Rechnungsbetrag wird vom Girokonto des Mobilfunkusers oder vom Kreditkartenkonto abgebucht. Der User hat aber auch die Möglichkeit, die Mobilfunkrechnung per Überweisung zu begleichen. Danach sendet der Mobilfunknetzbetreiber das Geld an die Bank des MCP mit dem Pseudonym des Users. Der gleicht dann die gelieferten Services anhand des Pseudonyms der User mit den Geldeinzahlungen bei seiner Bank ab.

Mit der Umsetzung eines solchen Mobile Payment Prozesses kann eine User-Anonymität im Mobile Payment Systemen realisiert werden. Für die Realisierung des Referenzprozessmodells müssen jedoch einige prozessuale Anpassungen bei den Prozessbeteiligten vorgenommen werden. Auf die Beantwortung der Fragen der Realisierung und der erforderlichen Prozessanpassungen wird im Kapitel 7 Gestaltungsmöglichkeiten der User-Anonymität in Mobile Payment Systemen (S. 169) eingegangen. Die Marktteilnehmer, insbesondere MCP und seine Bank, erhalten nach wie vor Transaktionsdaten, aber keine personenbezogenen Daten des Mobilfunkusers. Deshalb soll zunächst die User-Anonymität gegenüber den Marktteilnehmern im Referenzprozessmodell bewertet werden, indem die Verteilung der prozessnotwendigen Transaktionsdaten bzw. personenbezogenen Daten und Informationen zwischen den Marktteilnehmern erörtert wird.

6.4.2 Bewertung der User-Anonymität gegenüber den Marktteilnehmern im Referenzprozessmodell

Die Anonymität von mobilen Usern im Mobile Payment steht im dargestellten Referenzprozessmodell gegenüber den Interessen der anderen Marktteilnehmer im Vordergrund. Auf der anderen Seite bleiben auch die Interessen einzelner Marktteil-

nehmer bewahrt. Die Marktteilnehmer insb. der MCP können nach wie vor ihre Funktionen ausüben. Dazu werden die prozessnotwendigen Daten und Informationen der User jeweils unter den Marktteilnehmern verteilt. Deshalb soll im Folgenden die Verteilung der prozessnotwendigen Transaktionsdaten und Userdaten zwischen den Marktteilnehmern und die Anonymität von Usern gegenüber den anderen Marktteilnehmern detailliert erörtert werden.

6.4.2.1 User-Anonymität gegenüber dem Mobilfunknetzbetreiber

Der User ist der Kunde des Mobilfunknetzbetreibers. Seine Identität ist dem Mobilfunknetzbetreiber bekannt. Der mobile User kann unter besonderen Umständen gegenüber dem Mobilfunknetzbetreiber nicht anonym sein, da erstens der Mobilfunknetzbetreiber die ganze Netzwerk- und Telekommunikationsinfrastruktur zur Verfügung stellt, über die er dann die Identität und Kommunikation der mobilen User nachvollziehen kann. Zweitens kann der Mobilfunknetzbetreiber die IMEI-Gerätenummer, SIM-Kartennummer und Rufnummer den Usern einfach zuordnen. Drittens bietet und nutzt der Mobilfunknetzbetreiber seine Billing- und Payment-Infrastruktur zur Abwicklung von mobilen Kommunikations-, Billing- und Payment-Services. Somit hat der Mobilfunknetzbetreiber die Möglichkeit, jederzeit das Surf- und Kaufverhalten zu analysieren. Für den Mobilfunkuser existiert jedoch die Möglichkeit, seine Identität auch gegenüber dem Mobilfunknetzbetreiber zu verbergen. Diese Möglichkeit gibt es zumindest für die Ortanonymität des Users, wenn der User Location based Services nutzt und bezahlt.[547] Für die Ortanonymität des Users gibt es bereits Lösungsvorschläge. Nach diesen Vorschlägen kann sogar selbst der Mobilfunknetzbetreiber keine Bewegungsprofile vom Mobilfunkuser erstellen.[548]

6.4.2.2 User-Anonymität gegenüber dem Anonymitätsservice

Im dargestellten Referenzprozessmodell spielt der Anonymitätsservice eine Schlüsselrolle, da dieser die personenbezogenen Daten der User nicht überträgt und stattdessen anonymisierte Serviceanfragen der User an den MCP und die Bank des

---

[547] Vgl. mit den Erläuterungen für die Location based Services im Abschnitt 2.1.2 Location Based Services, S. 16 sowie die Erläuterungen für die Ortanonymität im Abschnitt 4.3.3 Ortanonymität, S. 97.

[548] Vgl. Federrath et al. (1997), S. 169ff.

MCP sendet. Der MCP und seine Bank erhalten keine personenbezogenen Daten wie z. B. die IMEI-Gerätenummer, SIM-Kartennummer und Rufnummer. Sondern können die anonymisierte mobile IP des Users bzw. des Anonymitätsservice sehen, wenn sie eine anonymisierte Serviceanfrage erhalten.

Die Anonymität des mobilen Users ist gegenüber dem Anonymitätsservice in der Regel nicht gegeben. Das heißt, die Identität des mobilen Users ist dem Anonymitätsservice bekannt. Jedoch ist die Bekanntheit der Identität des Users relativ. Das heißt, abhängig von der Anwendung des jeweiligen Anonymitätskonzeptes ist die User-Anonymität unterschiedlich gewährt. Beispielsweise bei einer Anwendung des Mix-Konzeptes weiß der erste Mix-Server zwar, wer die Serviceanfrage gesendet hat.[549] Jedoch erfährt er weder etwas über den Empfänger, noch über den Inhalt der verschlüsselten Serviceanfrage. Auf der anderen Seite kennt der letzte Mix-Server zwar den Empfänger der Serviceanfrage, kann aber den Sender der Serviceanfrage nicht erfahren. Mittlere Mix-Server kennen nur den Vorgänger-Mix-Server und den Nachfolger-Mix-Server. Somit können Sender und Empfänger einer Serviceanfrage nicht miteinander in Verbindung gebracht werden. Der mobile User hat damit die Senderanonymität.[550]

6.4.2.3 User-Anonymität gegenüber dem Mobile Content Provider

Der Mobile Content Provider (MCP) ist der Marktteilnehmer, gegenüber dem der mobile User als Kunde anonym shoppen und bezahlen möchte. Im allgemeinen Mobile Payment Prozess erhalten MCP in der Regel fast alle personenbezogenen Daten des mobilen Users. Im dargestellten Referenzprozessmodell kann jedoch der mobile User gegenüber dem MCP mit verschiedenen Graden der Anonymität auftreten.[551] Danach hat der mobile User drei Möglichkeiten, wenn er Mobile Content herunterlädt, um seine Identität gegenüber dem MCP steuern zu können:

- Erstens kann der mobile User seine Identität gegenüber dem MCP offenlegen. Hier besteht keine User-Anonymität.

---

[549] Vgl. mit dem Abschnitt 5.2.4 Anonymitätskonzepte sowie mit dem Abschnitt 5.2.4.4 Mixe und deren Anwendung in der Praxis, S. 124ff.

[550] Vgl. mit dem Abschnitt 4.3 Formen der Anonymität, S. 88 sowie mit dem Abschnitt 4.3.1.1 Senderanonymität, S. 91.

[551] Die Grade der Anonymität werden im Abschnitt 4.4 Identität und Grade der Anonymität, S. 98 ausführlich erläutert.

- Zweitens kann der User seine Identität gegenüber dem MCP nur teilweise verbergen. Er kann mit Hilfe der Pseudonymisierung seine Identität teilweise verbergen.

- Drittens kann der User seine Identität gegenüber dem MCP unter absoluter Anonymität ganz verbergen.

Der mobile User hat diese Möglichkeiten und kann seine Identität und Anonymität gegenüber dem MCP selber bestimmen. Auf diese Weise können MCP die Identität des Mobilfunkusers nicht erkennen. Sie können weder die Einkäufe des Users noch dessen Aufenthaltsort miteinander verketten und Nutzungs- und Bewegungsprofile des mobilen Users erstellen. Bei der Anwendung der Pseudonymisierung kennen MCP unter bestimmten Bedingungen nur die Teilidentität des Users.[552] Damit kann der mobile User eine partielle Anonymität erlangen.

6.4.2.4 User Anonymität gegenüber der Trusted Third Party

Die Rolle der Trusted Third Party ist die Durchführung der Authentifizierung und Autorisierung der Prozessbeteiligten.[553] Deshalb ist die TTP im Referenzprozessmodell als vertrauenswürdige Instanz integriert, um die Sicherheit und das Vertrauen im Mobile Payment für alle Prozessbeteiligten zu schaffen. Im Referenzprozessmodell kann die TTP die Identität des Mobilfunkusers anhand des bei ihm hinterlegten öffentlichen Schlüssels erkennen, mit dem sie die Anonymität des Users aufheben kann (Rückverfolgbarkeit des Users). Daher ist der mobile User gegenüber der TTP nicht anonym. Diese Tatsache erfordert, dass die TTP als Vertrauensinstanz unabhängig von den Marktteilnehmern agiert. Die Unabhängigkeit der TTP ist deshalb wichtig und für das Funktionieren des organisatorischen Konzeptes für die User-Anonymität vorausgesetzt. Wenn es zu einer Ermittlung oder Strafverfolgung kommt, dann erfolgt die Aufhebung der Anonymität nur gegenüber den Justizbehörden. Daher darf die TTP die Offenlegung des bei ihr hinterlegten Schlüssels nur gegenüber den Justizbehörden machen.

---

552 Die Erläuterungen über die Teilidentität und Pseudonyme erfolgen im Abschnitt 4.4.2 Teilidentität - Pseudonymität - Partielle Anonymität, S. 102.

553 Die Rolle der Trusted Third Party werden im Abschnitt 3.1.7 Trusted Third Party, S. 60 detailliiert beschrieben.

6.4.2.5 User Anonymität gegenüber dem Staat

Der Mobilfunkuser hat die Möglichkeit, auch gegenüber dem Staat anonym zu bleiben, ohne dabei seine Rechte und Pflichten missbraucht bzw. verletzt zu haben und kriminell zu werden. Nur bei kriminellen Aktivitäten und Strafverfolgungen darf der Staat die Möglichkeit haben, die Anonymität des Users aufzuheben.[554] Im Referenzprozessmodell hat der Staat die Rolle, die regulatorischen Maßnahmen für das Funktionieren des anonymen Mobile Payments zu treffen. Im Referenzprozess-modell erhält der Staat zunächst keine personenbezogenen bzw. Verbindungsdaten. Daher bleibt der User im Referenzprozessmodell gegenüber dem Staat mit Vorbehalt vorerst anonym.

Im nächsten Kapitel werden die Gestaltungsmöglichkeiten der User-Anonymität in Mobile Payment Systemen ausführlich erklärt.

[554] Die Rolle und Interessen vom Staat wird im Abschnitt 3.1.8 Staat, S. 62 näher erklärt.

7 Gestaltungsmöglichkeiten der User-Anonymität in Mobile Payment Systemen

Nach dem das Referenzprozessmodell für die Gestaltung der User-Anonymität dargestellt und die User-Anonymität gegenüber den Marktteilnehmern bewertet wurden, werden in diesem Kapitel die Gestaltungsmöglichkeiten der User-Anonymität anhand der bereits dargestellten Anforderungen und Rahmenbedingungen der Anonymität gezeigt werden. Hierfür werden die Maßnahmen und Handlungsmöglichkeiten sowie Handlungsempfehlungen zur Herstellung und Bewahrung der User-Anonymität dargestellt. Außerdem werden die potentiellen Risiken und Probleme sowie Fragen, die bei der Gestaltung der User-Anonymität auftauchen können, und deren Lösungsmöglichkeiten gezeigt. Dies wird in drei Schritten mit folgenden Analysen erläutert:

- im ersten Schritt werden die Anforderungen an einen anonymen Mobile Payment Prozess analysiert, in wie fern diese Anforderungen im Referenzprozessmodell berücksichtigt und erfüllt werden können. Hierfür werden die Berücksichtigung und Erfüllung der allgemeinen, technischen, funktionalen und wirtschaftlichen Anforderungen sowie der Anforderungen von Marktteilnehmern im anonymen Mobile Payment Prozess erläutert.
- im zweiten Schritt werden die Rahmenbedingungen für den anonymen Mobile Payment Prozess analysiert werden, in wie fern die Rahmenbedingungen für den anonymen Mobile Payment Prozess im Referenzprozessmodell berücksichtigt und erfüllt werden können bzw. welche Rahmenbedingungen noch angepasst werden sollten. Hierfür werden die Berücksichtigung und Erfüllung der organisatorischen, technischen und regulatorischen Rahmenbedingungen für den anonymen Mobile Payment Prozess erklärt.
- Im dritten und letzten Schritt werden die potentiellen Risiken und Probleme sowie Fragen im anonymen Mobile Payment Prozess erläutert, welche Maßnahmen und Regelungen dafür erforderlich sind. Hierfür werden die Hinweise auf die organisatorischen, technischen und regulatorischen Risiken und Probleme sowie deren Maßnahmen und Lösungsmöglichkeiten gegeben.

7.1 Berücksichtigung und Erfüllung von Anforderungen

Welche Interessen einzelne Marktteilnehmer im Mobile Payment System verfolgen und welche Anforderungen die Marktteilnehmer an den Mobile Payment System stellen bzw. welche Anforderungen zu erfüllen sind, wurde bereits in den vorigen Ab-

schnitten gezeigt.[555] Nun soll gezeigt werden, in wie fern die Anforderungen der Marktteilnehmer im Referenzprozessmodell berücksichtigt und erfüllt werden können. Zu diesem Zweck werden die kritischen Merkmale des Referenzprozessmodells gezeigt und analysiert, in wie fern die Anforderungen der Marktteilnehmer im anonymen Mobile Payment System erfüllt werden können. Im Folgenden werden die Berücksichtigung und Erfüllung der

- allgemeinen Anforderungen
- technischen Anforderungen
- funktionalen und wirtschaftlichen Anforderungen sowie
- Anforderungen der Marktteilnehmer insb. User und Händler

im Referenzprozessmodell gezeigt.

7.1.1 Berücksichtigung und Erfüllung von allgemeinen Anforderungen

Bei der Gestaltung des Referenzprozessmodells sollen die allgemeinen Anforderungen an Mobile Payment Systemen berücksichtigt werden.[556] Zunächst sollen die anonymen Zahlungstransaktionen in anonymen Mobile Payment Prozess vollständig sichergestellt werden. Wenn ein anonymes Mobile Payment durchgeführt wird, soll der ganze anonyme Mobile Payment Prozess vollständig sicher sein. Im Referenzprozessmodell kann diese Anforderung durch die Nutzung der Anonymitätskonzepte und Verschlüsselungstechniken erfüllt werden.

Die Integrität der Zahlungsdaten und -informationen soll auch beim anonymen Mobile Payment gewährleistet sein. Dabei ist zu verstehen, dass die erhaltenen Daten und Informationen des Users bzw. der Transaktion vollständig und unverändert über einen bestimmten Zeitraum bewahrt werden sollen. Bei der Anonymisierung kann diese Anforderung nur teilweise erfüllt werden, da die Userdaten bei einer Serviceanfrage durch den Anonymitätsservice anonymisiert und so übertragen werden, während die Verbindungs- bzw. Transaktionsdaten der Serviceanfrage unverändert und vollständig übertragen werden können.

---

[555] Die Interessen und Anforderungen von einzelnen Teilnehmern werden im Abschnitt 3.2 Interessen und Anforderungen der Marktteilnehmer, S. 63ff. ausführlich behandelt.

[556] Die allgemeinen Anforderungen an Mobile Payment Systemen werden im Abschnitt 3.2.1 Allgemeine Anforderungen, S. 63 erläutert.

Die Unabhängigkeit von Zahlungstransaktionen kann im Referenzprozessmodell gewährleistet werden, da die Zahlungstransaktionen anonym durchgeführt werden und sich dadurch untereinander nicht beeinflussen können. Anders würde die Gefahr der Verkettung von Zahlungstransaktionen bestehen. Im Referenzprozessmodell kann die Dauerhaftigkeit von Zahlungsinformationen bei Verlust, Diebstahl oder Missbrauch gewährleistet werden, da sowohl der Mobilfunknetzbetreiber und als auch der Anonymitätsservice diese Dauerhaftigkeitsanforderung erfüllen können. Unmittelbar damit hängt die Reputation und Verlässlichkeit der anonymen Mobile Payment Systeme zusammen. Im Referenzprozessmodell ist die Vertrauenswürdigkeit und Dauerhaftigkeit durch die Vertrauensinstanzen und den Anonymitätsservice gegeben, da die Authentifizierung der Marktteilnehmer mit den Verschlüsselungstechniken, digitalen Zertifikaten sowie Anonymitätstechniken gewährleistet werden kann.

Die Anforderungen der Allgegenwärtigkeit bzw. der permanenten Verfügbarkeit sollen in einem anonymen Mobile Payment System berücksichtigt werden. Im Referenzprozessmodell können diese Anforderungen gewährleistet werden, da mobile User nach wie vor wie in klassischen Mobile Payment Prozessen zeit-, und ortunabhängig mit ihren Mobilfunkgeräten anonym einkaufen und bezahlen können.

Der Datenschutz sowie die Privatsphäre sollen in einem anonymen Mobile Payment System berücksichtigt werden. Diese Anforderung kann im Referenzprozessmodell gewährleistet werden. Mit Hilfe des Anonymitätsservices kann der mobile User selber über die Preisgabe und Verwendung seiner personenbezogenen Daten entscheiden. Außerdem erhalten die Marktteilnehmer im Referenzprozessmodell nur pseudonymisierte bzw. anonymisierte Daten des Users.

Die Anforderung der Internationalität von anonymen Mobile Payment Systemen kann insofern erfüllt werden, wie dies in Mobile Payment Systemen in Deutschland und den anderen Ländern unterstützt werden kann. Die Anforderung des Entwicklungspotentials von Mobile Payment Systemen ist im Referenzprozessmodell gegeben und daher besitzt das Referenzprozessmodell ein großes Potenzial für die Entwicklung weiterer anonymen Zahlungsprozesse. Das bedeutet, dass die User-Anonymität einen großen Nutzen in Mobile Payment Systemen und somit große Akzeptanz bei den Usern bietet.

7.1.2 Berücksichtigung und Erfüllung von technischen Anforderungen

Die technischen Anforderungen betreffen die sicherheits-, integrations- und realisierungsrelevanten Anforderungen.[557] Die Sicherheitsanforderungen der Verfügbarkeit und Zuverlässigkeit von Mobile Payment Systemen sollen bei der Realisierung des Referenzprozessmodells berücksichtigt werden. Daher sollen die Mobile Payment Systeme jederzeit verfügbar sein und zuverlässig funktionieren, wenn der User das anonyme Mobile Payment nutzt. Die Transaktionsdaten und -informationen sollen nur den jeweiligen Prozessbeteiligten bekannt sein und vertraulich behandelt werden. Personenbezogene Daten sind nur dem Mobilfunknetzbetreiber und zusätzlich auch dem Anonymitätsservice abhängig von der Anwendung des jeweiligen Anonymitätskonzeptes bekannt. Außerdem soll berücksichtigt werden, dass die Transaktionsdaten und Informationen unverändert übertragen werden, wobei der User anonym bleiben soll. Diese Anforderung kann erfüllt werden, wenn die Transaktionsdaten getrennt von den personenbezogenen Daten übertragen werden können.[558]

Die Anforderungen der Authentisierung und Autorisierung des Users bzw. der Servicelieferung spielen eine zentrale Rolle im Referenzprozessmodell. So werden die Prozessbeteiligten durch ein Verifizierungsverfahren gegenseitig identifiziert. Im Referenzprozessmodell soll die Authentifizierung des Users durch die Public Key Infrastrukturen, Anonymitätsservice und TTP durchgeführt werden, so dass die Identifizierung des Users anhand eines bei der TTP hinterlegten öffentlichen Schlüssels erfolgt.[559] Gleichzeitig soll die Autorisierung des Users und Services erfolgen, bei der ein unberechtigter Zugriff auf die Transaktionsdaten verhindert wird. Die Non-Repudiation erfordert zwar eine eindeutige Identifizierung des Users, jedoch kann diese Anforderung durch die Identifizierung des Users anhand der TTP anonym erfüllt werden. Die Anforderung Schutz gegen die Angriffe können der Anonymitätsservice und die TTP bieten. Zwar sind die Angriffe von Dritten an dem Anonymitätsservice möglich, jedoch bieten die einzelnen Anonymitätskonzepte genügend Schutz.[560]

---

[557] Die technischen Anforderungen werden im Abschnitt 3.2.2 Technische Anforderungen, S. 65 erläutert.

[558] Vgl. mit den Erläuterungen im Abschnitt 7.3.1 Trennung der personenbezogenen Daten von den Transaktionsdaten, S. 179.

[559] Vgl. mit den Erläuterungen über die Verschlüsselungstechniken wie Public Key Infrastrukturen im Abschnitt 3.1.7 Trusted Third Party, S. 60.

[560] Vgl. mit den Erläuterungen im Abschnitt 5.2.4 Anonymitätskonzepte, S. 124ff.

Die Integrations- und Realisierungsanforderungen sollen ebenfalls im Referenzprozessmodell berücksichtigt bzw. erfüllt werden. Die Anforderungen betreffen technische Integrationsfähigkeit, Einfachheit und Sicherheit. Das Referenzprozessmodell kann sich in die vorhandenen, userspezifischen Applikationen und betriebliche IT-Infrastrukturen einfach integrieren lassen. Auf die Integration der notwendigen prozessualen Änderungen im Referenzprozessmodell wird im nächsten Kapitel eingegangen.[561] Der User selbst installiert dafür entweder eine spezielle Applikation des Anonymitätsservices oder setzt über den WAP-Service des Anonymitätsservices seinen Einkauf und seine Zahlung fort. Bei den anonymen Zahlungstransaktionen soll es akzeptable Datenverarbeitungsgeschwindigkeiten geben, so dass die Transaktionskosten niedrig bleiben.

7.1.3 Berücksichtigung und Erfüllung von funktionalen und wirtschaftlichen Anforderungen

Bei der Gestaltung des Referenzprozessmodells sollen die funktionalen und wirtschaftlichen Anforderungen berücksichtigt und erfüllt werden.[562] Wenn der mobile User einen Anonymitätsservice in einem Mobile Payment System benutzen möchte, sollen diese eine bestimmte Systemoffenheit bieten, damit ein Zugang zu einem anonymen Mobile Payment System für die Marktteilnehmer möglich ist. Zwar soll der User eine spezielle Software für den Anonymitätsservice nutzen, jedoch sollte dies freizugänglich für alle User sein, damit sie diese spezielle Applikation in ihr Mobilfunkgerät ohne ein Problem installieren und nutzen können. Die elektronischen Zahlungsdaten und -informationen von Usern und Händlern sollen entsprechend dem Referenzprozessmodell und den gesetzlichen Rahmenbedingungen gespeichert werden, um gegen möglichen Verlust, Diebstahl und Missbrauch zu schützen. Bei der Speicherung und Nutzung von Userdaten sollen die personenbezogenen Daten von den Verbindungs- bzw. Transaktionsdaten getrennt und auf dieser Weise anonym gespeichert werden. Die personenbezogenen Daten wie Username, -adresse und Kreditkartennummer sollen verschlüsselt in einem separaten Server außerhalb des Internets gespeichert werden.[563] Bei der Realisierung des Referenzprozessmodells sollen auch die Gebühren und Transaktionskosten für die Nutzung

---

[561] Vgl. mit den Erläuterungen im Abschnitt 7.3.6 Erforderliche Prozessanpassungen seitens der Markteilnehmer, S. 185.

[562] Die funktionalen und wirtschaftlichen Anforderungen werden im Abschnitt 3.2.3 Funktionale und wirtschaftliche Anforderungen, S. 70 ausführlich behandelt.

[563] Dieses Thema wird im Abschnitt 7.3.1 Trennung der personenbezogenen Daten von den Transaktionsdaten, S. 179 näher erläutert.

des Anonymitätsservices und Installation bzw. Update der speziellen Applikation berücksichtigt werden, wobei die Attraktivität der Nutzung eines Anonymitätsservice für die User hoch bleibt. Für die Nutzung des Anonymitätsservices sowie der Applikation können Entgelte erhoben werden. Alternativ könnte dieser Anonymitätsservice werbefinanziert genutzt werden. Jedoch ließe dies sich nicht ohne Bedenken realisieren, da dies zu Lasten der Anforderung der Unabhängigkeit des Anonymitätsservice bzw. Vertrauen der User gehen könnte. In welcher Höhe die Kosten durch die Nutzung eines Anonymitätsservices anfallen würden, kann in diesem Stadium nicht gesagt werden, da dies in einer geringfügigen Höhe und erst in der Praxis überprüft werden sollte. Ein anonymes Mobile Payment System soll die Eignung für alle Art der Einkäufe haben. Diese Anforderung kann für das Beispiel Mobile Content Download im Referenzprozessmodell erfüllt werden, so dass der mobile User seine Anonymität bei der Nutzung von Mobile Content Download im Referenzmodell managen kann.

7.1.4 Berücksichtigung und Erfüllung von Anforderungen der mobilen Usern

Bei der Gestaltung des Referenzprozessmodells sollen die Anforderungen von mobilen Usern in vollem Maße berücksichtigt und erfüllt werden.[564] Die erste Anforderung ist der Schutz der personenbezogenen Daten und Informationen vor einem Missbrauch bzw. vertraulicher Umgang mit den personenbezogenen Daten. Da diese Anforderung im Referenzprozessmodell eine zentrale Bedeutung hat, soll eine kontrollierbare User-Anonymität ermöglicht werden. Das heißt, wenn der mobile User mit seinem Mobilfunkgerät surft, einkauft und bezahlt, soll er in der Lage sein, selber zu entscheiden, ob er anonym tun möchte. Wenn der User anonym surfen möchte, soll er dies über einen Anonymitätsservice tun können. Auf dieser Weise sollen bei einer Zahlungstransaktion keine personenbezogenen Daten an die Prozessbeteiligten übertragen werden. Damit ist es möglich, die Anforderung, dass die personenbezogenen Daten vor Missbrauch geschützt und damit vertraulich umgegangen werden soll, im Referenzprozessmodell zu erfüllen.

Die Anforderung der Userfreundlichkeit soll bei der Realisierung des Referenzprozessmodells dadurch erfüllt werden, dass der User mit dem Mobilfunkgerät automatisch oder manuell einen Anonymitätsservice wählen kann. Dies kann beispielsweise durch eine spezielle Applikation für das Identitätsmanagement auf dem Mobil-

[564] Die Anforderungen der mobilen User werden im Abschnitt 3.2.4.1 Anforderungen der mobilen User, S. 72 ausführlich behandelt.

funkgerät des Users oder durch die Bereitstellung eines Web-Applikation des Anonymitätsservice realisiert werden. Eine einfache und intuitive Bedienung des Anonymitätsservices erhöht damit die Attraktivität und Akzeptanz eines Mobile Payment Systems bei den Usern. Die Anforderung Vertrauen kann bei der Realisierung des Referenzprozessmodells neben dem Anonymitätsservice durch die TTP gewährleistet werden, die die Authentifizierung des Users und die Autorisierung des Services ermöglicht. Durch die Public Key Verschlüsselung bzw. digitale Signaturen werden die User und deren Transaktionen zertifiziert. Die TTP zertifiziert ebenfalls die Identität der Händler und MCP und schafft dadurch Vertrauen zwischen Usern und Händlern. Durch das Referenzprozessmodell ist es mobilen Usern möglich, zeit-, ort- und währungsunabhängig zu bezahlen. Bei der Realisierung des Referenzprozessmodells soll berücksichtigt werden, dass diese Anforderung der Ubiquität (Allgegenwärtigkeit) der anonymen Mobile Payments erfüllt wird, da der User in unterschiedlichen Situationen wie beim Parken, bei Reisen oder in der Freizeit etc. sein Mobilfunkgerät einsetzen und mobil bezahlen möchte.

Die Kosten könnten unter Umständen in Form der Nutzungsgebühren für die kostenpflichtige Nutzung des Anonymitätsservice entstehen, wenn es dafür unabhängige und kommerzielle Anbieter bzw. Angebote geben würde. Allerdings sollten diese Nutzungsgebühren so niedrig sein, dass die Attraktivität der Nutzung des anonymen Mobile Payment Systems nicht beeinträchtigt wird. Dies kann beispielsweise auch als ein kostenloser Anonymitätsservice z. B. als ein Value-Added-Service von Mobilfunknetzbetreibern oder anderen Institutionen angeboten werden.[565] Bei der Nutzung eines solchen Anonymitätsservices kann der User eine spezielle Software (ähnlich wie JAP-Software) installieren oder sein Mobilfunkgerät entsprechend konfigurieren.[566]

7.1.5 Berücksichtigung und Erfüllung von Anforderungen des Händlers

Bei der Gestaltung der User-Anonymität im Referenzprozessmodell sollen die Interessen und Anforderungen von Händlern bzw. Mobile Content Provider berücksichtigt bzw. erfüllt werden, welche sich naturgemäß von denen des mobilen Users

[565] Vgl. dazu auch die Erläuterungen über den Anonymitätsservice im Abschnitt 7.3.3 Einrichtung eines Anonymitätsservices, S. 182.

[566] Vgl. dazu auch die Erläuterungen im Abschnitt 7.3.6.1 Prozessanpassungen und Ausstattung der User, S. 185.

unterscheiden.[567] Für die Händler ist wichtig, dass die Transaktionskosten im anonymen Mobile Payment System niedrig sind, ein geringes bis gar kein Betrugs- und Zahlungsausfallrisiko vorhanden und geringer technischer Aufwand für die Integration in die eigenen Geschäftsprozesse erforderlich ist. Im Referenzprozessmodell entstehen für die Händler keine zusätzlichen Transaktionskosten, da der Wunsch der Anonymität von Seiten der User kommt und die möglichen Kosten der User-Anonymität unter Umständen von Usern selbst zu tragen sind. Die Händler haben in Betrugsfällen normalerweise keine oder unzureichende Mittel gegenüber dem (betrügerischen) User. Die erforderliche Zahlungssicherheit für die Händler kann jedoch durch die Authentifizierung der User und die Autorisierung des Services durch die TTP und Mobilfunknetzbetreiber gewährleistet werden. Die Integration eines anonymen Mobile Payment Systems bei Händlern wie im Referenzprozessmodell stellt kein großes Problem dar, da der Tausch der Transaktionsdaten zwischen den Händler-Servern und Anonymitätsservice-Servern wie in einem allgemeinen Mobile Payment Prozess reibungslos läuft. Die Händler erhalten im Referenzprozessmodell nach wie vor die für ihre Geschäfte nötigen Transaktionsdaten, jedoch ohne personenbezogene Daten von mobilen Usern.

Außerdem würden die Händler gerne ihre Kunden hinsichtlich ihres Kaufverhaltens oder ihrer Persönlichkeit durchschauen. Dafür würden die Händler einfach die Transaktionsdaten und personenbezogenen Daten analysieren. Der Nachteil für die Händler kann darin bestehen, dass sie bei anonymen Mobile Payments keine interessanten Angebote oder Vergünstigungen für ihre Stammkunden machen können. Jedoch gibt es auch in so einem Fall die Möglichkeit, einen gewissen Grad an Anonymität anzubieten. Beispielsweise kann die Pseudonymität als eine abgeschwächte Form der Anonymität angeboten werden.[568] Im Referenzprozessmodell ist zwar eine Analyse der Transaktionen durch die Händler bzw. MCP nach wie vor möglich. Da die Händler nicht mehr personenbezogene Daten erhalten, können sie die Transaktionsdaten zu den Usern nicht zuordnen. Sie wissen also nicht, wer bei ihnen kauft bzw. bezahlt. Die Händler liefern das Produkt oder den Service an den User und bekommen ihr Geld.

---

[567] Die Anforderungen der Händler werden im Abschnitt 3.2.4.2 Anforderungen der Händler, S. 75 ausführlich behandelt.

[568] Vgl. mit den Erläuterungen im Abschnitt 4.4.2 Teilidentität - Pseudonymität - Partielle Anonymität, S. 102.

7.1.6 Berücksichtigung und Erfüllung von Anforderungen anderer Teilnehmern

Bei der Gestaltung der User-Anonymität im Referenzprozessmodell sollen die Anforderungen von Mobilfunknetzbetreibern, Trusted Third Parties, Banken und vom Staat berücksichtigt bzw. erfüllt werden.

Die Mobilfunknetzbetreiber interessieren sich vor allem dafür, dass der User sein Mobilfunkgerät möglichst lange „on air“ nutzt. Das heißt, dass der User sein Mobilfunkgerät für die Telekommunikationsdienste und die Services von Dritten (z. B. Mobile Content Provider) einsetzt, damit der Mobilfunknetzbetreiber mehr Umsatz generieren kann. Daher braucht der Mobilfunknetzbetreiber nur zu wissen, welcher mobile User, welche Services von wem bzw. welchen MCP bezogen hat, damit er diese Services abrechnen kann. Der Mobilfunknetzbetreiber kann für die Abrechnung dieser Services die Möglichkeit der Anonymisierung bzw. Pseudonymisierung der personenbezogenen Daten nutzen, die ja auch per Gesetz geboten werden. Deshalb soll diese Anforderung von Mobilfunknetzbetreiber bei der Gestaltung der User-Anonymität berücksichtigt werden.

Trusted Third Parties haben Interesse daran, dass die Authentifizierung bzw. Identifizierung der Marktteilnehmer gegenseitig auf einer Vertrauensbasis geschieht. Für die Erfüllung dieser Aufgabe brauchen die TTP, die Userdaten und die Daten der anderen Prozessbeteiligten. Daher soll auch diese Anforderung berücksichtigt werden. Die Banken bzw. Kreditkartengesellschaften benötigen die Daten und Informationen, auf welches Konto sie überweisen bzw. welche Lastschriften sie einziehen dürfen, wobei sie keine personenbezogenen Daten der User brauchen. Die Bank des Händlers erhält das Geld von der Bank des Mobilfunknetzbetreibers mit einem pseudonymisierten Verwendungszweck. Der Staat hat Interesse daran, dass für die möglichen Gefahren und Risiken wie Geldwäsche, Betrug und andere Kriminalitäten durch die anonymen Mobile Payment Prozesse nicht Tür und Tor geöffnet werden. Bei der Gestaltung der User-Anonymität im Referenzmodell kann eine rückverfolgbare Anonymität ermöglicht werden. Beispielsweise im Streitfall oder in der Strafverfolgung kann die Identität des mobilen Users aufgedeckt werden. Daher

soll der Staat die Maßnahmen und Regelungen gegen die möglichen Gefahren und Risiken wie Geldwäsche, Betrug und andere Kriminalitäten ergreifen.[569]

Zusammenfassend kann festgehalten werden, dass für eine erfolgreiche Umsetzung eines anonymen Mobile Payment Prozesses in erster Linie die Anforderungen von mobilen Usern und Händlern als primäre Marktteilnehmer berücksichtigt bzw. erfüllt werden sollen. Nach der Analyse der Berücksichtigung und der Erfüllung von Anforderungen der mobilen Usern und Händlern sowie anderen Prozessbeteiligten soll im folgenden Abschnitt analysiert und erörtert werden, welche Rahmenbedingungen für die Gestaltung der User-Anonymität in Mobile Payment Systemen vorhanden sind bzw. geschaffen werden sollen.

7.2 Berücksichtigung von Rahmenbedingungen

Bei der Gestaltung der anonymen Mobile Payment Prozesse sollen die organisatorischen, technischen und rechtlichen Rahmenbedingungen berücksichtigt werden, damit die Anforderungen der Geschäftsprozesse und der Marktteilnehmern im anonymen Mobile Payment System erfüllt werden können.[570] Dafür können die vorhandenen Rahmenbedingungen ausgeschöpft bzw. neue für die reibungslose Funktion der User-Anonymität nötige Rahmenbedingungen geschaffen werden. Deshalb werden in folgenden Abschnitten die Gestaltungsmöglichkeiten der User-Anonymität in den Rahmenbedingungen gezeigt:

- Organisatorische Gestaltungsmöglichkeiten
- Technische Gestaltungsmöglichkeiten
- Regulatorische Gestaltungsmöglichkeiten

Zunächst werden die Gestaltungsmöglichkeiten bzw. die erforderlichen organisatorischen Rahmenbedingungen der anonymen Mobile Payment Systeme erörtert.

---

[569] Die Anforderungen und Interessen vom Staat werden bei den regulatorischen Gestaltungsmöglichkeiten berücksichtigt. Dies wird im Abschnitt 5.3 Regulatorische Gestaltungsmöglichkeiten, S. 199 näher erläutert.

[570] Die organisatorischen, technischen und regulatorischen Rahmenbedingungen der Anonymität werden im Kapitel 5 Rahmenbedingungen der User-Anonymität, S. 113ff. ausführlich behandelt.

7.3 Organisatorische Gestaltungsmöglichkeiten

Für die organisatorische Gestaltung der anonymen Mobile Payment Systeme und Prozesse sollen die vorhandenen organisatorischen Rahmenbedingungen genutzt bzw. neu geschaffen werden. Wie schon im Abschnitt 5.1 Organisatorische Rahmenbedingungen der User-Anonymität, S. 113 erläutert wurde, geht es bei der organisatorischen Gestaltung um die Organisation und Verbesserung der Geschäftsprozesse sowie die Verteilung und der Schutz der darin fallenden Daten und Informationen. Deshalb umfasst die organisatorische Gestaltung des im Referenzprozessmodell dargestellten anonymen Mobile Payment Systems die folgenden organisatorischen Gestaltungsmöglichkeiten:

- die Trennung von personenbezogenen Daten von den Transaktionsdaten
- die Berücksichtigung der Besonderheiten digitaler und physischer Produkte
- die Einrichtung eines Anonymitätsservices
- die Einrichtung einer Trusted Third Party
- die erforderlichen Anpassungen seitens der Prozessbeteiligten

In den folgenden Abschnitten werden diese notwendigen organisatorischen Gestaltungsmöglichkeiten ausführlich behandelt.

7.3.1 Trennung der personenbezogenen Daten von den Transaktionsdaten

Die Grundidee bei der Gestaltung eines anonymen Mobile Payment Prozesses ist die Trennung der personenbezogenen Daten von den Transaktionsdaten.[571] Auf dieser Weise sollen die Prozessbeteiligten keine unnötigen Daten für die Abwicklung der Geschäftstransaktionen erhalten. Deshalb soll berücksichtigt werden, dass die User-Anonymität dadurch hergestellt werden kann, wenn die personenbezogenen Daten bei einer Kauf- bzw. Zahlungstransaktion von den Transaktionsdaten getrennt werden können. Dabei soll beachtet werden, dass die Funktion der Geschäftsprozesse im anonymen Mobile Payment System dabei nicht beeinträchtigt werden sollte. Das heißt, dass jeder Marktteilnehmer nur die Daten des mobilen Users bekommt, die auf ihrer Seite für die Abwicklung des Geschäftes bzw. der Mobile

[571] Die Definition und Organisation der Daten wird im Abschnitt 5.1 Organisatorische Rahmenbedingungen der User-Anonymität, S. 113 und im Abschnitt 5.1.2 Bestandsdaten und personenbezogene Daten, S. 117 sowie im Abschnitt 5.1.4 Verbindungsdaten und Transaktionsdaten, S. 119 ausführlich behandelt.

Payment notwendig sind. Dabei soll jeder Marktteilnehmer unter dem Aspekt des Gesetzesgebots „Datenvermeidung“ und „Datensparsamkeit“ handeln und ihre Geschäftsprozesse unter diesem Aspekt errichten. Das bedeutet, dass die Marktteilnehmer keine unnötigen Daten des Users auf Dauer speichern und verwenden. Beispielsweise soll der MCP keine personenbezogenen Daten des Mobilfunkusers erhalten, sondern nur die Serviceanfrage mit den gewünschten Produktoptionen, anonymisierte Userdaten und -information und eine Lieferschnittstelleninformation, auf die im nächsten Abschnitt näher eingegangen wird.

7.3.2 Berücksichtigung der Besonderheiten digitaler und physischer Produkten

Bei der Gestaltung eines anonymen Mobile Payment Prozesses sollen einige Besonderheiten bei digitalen und physischen Produkten insb. bei der Lieferung dieser Produkte und Services berücksichtigt werden.[572] Bei der Lieferung der digitalen und physischen Produkte an den mobilen User bzw. die Adresse des mobilen Users gibt es den entscheidenden Unterschied, der die Anonymität des Users beeinträchtigt. Während die Lieferung bei digitalen Produkten an das Mobilfunkgerät des Users erfolgt, wird das physische Produkt an die Anschrift bzw. Wohnadresse des Users geliefert oder am POS im Geschäft persönlich ausgehändigt oder am Verkaufsautomat ausgegeben. Auf diese Weise können sowohl MCP als auch Händler die gelieferten Produkte den Kunden zuordnen. Somit sind sie in der Lage, alle Kaufvorgänge zu verketten und Profile von ihren Kunden zu erstellen, wie dies beim Data Mining im Marketing durchgeführt wird.[573]

Bei der Lieferung der digitalen Inhalte und Services braucht der MCP die Mobilfunknummer des Users. Erst wenn die Mobilfunknummer an den Content Provider mitgeteilt ist, kann er das Produkt oder den Service an den Kunden liefern. Beispielsweise sendet der MCP eine SMS mit einem Link. Der Mobilfunkuser bestätigt dies mit einem SMS gesendeten Link. Es wird dann eine Verbindung zum Mobilfunkgerät hergestellt, bei der die Mobilfunk- und Mobilfunkgerätenummer und die IP-Adresse

---

572 Digitale und physische Produkte und Services werden im Abschnitt 2.4 Mobile Payment Typen, S. 23 und im Abschnitt 2.7 Anwendungsbereiche von Mobile Payments, S. 41. Vgl. dazu auch die Abbildung 4, S. 25, in der ein Überblick über die digitale und physische Produkte und Services mit Beispielen gegeben ist.

573 Vgl. mit den Erläuterungen über Data Mining im Abschnitt 5.1.5 Behandlung der Verbindungs- und Transaktionsdaten, S. 120.

des Users übermittelt werden. Somit ist der Content Provider in der Lage, die bestellten Produkte zu den Mobilfunkgeräten zuzuordnen bzw. deren Inhaber zu identifizieren.

Mit dem dargestellten anonymen Mobile Payment Prozess soll der Mobilfunkuser in der Lage sein, anonym einkaufen und bezahlen zu können. Wenn der Mobilfunkuser seine Identität bewahren möchte, surft und kauft er beim MCP und zahlt anonym, indem er einen Anonymitätsservice nutzt. Welche Daten und Informationen braucht der MCP mindestens, damit er das Produkt bzw. den Service an den Mobilfunkuser liefern kann? Der MCP braucht eine Mobilfunknummer des Users als Mindestinformation für die Lieferung digitaler Inhalte. Diese Lieferung erfolgt in der Regel als Premium SMS- oder MMS-Format. Er bekommt eine Mobilfunknummer, an die er liefern kann, die jedoch zuvor durch einen Anonymitätsservice anonymisiert werden sollte. Wenn der Mobilfunkuser nochmals beim gleichen Content Provider einen Service nutzt, soll der Content Provider jedes Mal eine andere Mobilfunknummer bekommen. Dies kann beispielsweise unter Umständen mittels der Einweg-Pseudonyme realisiert werden. Das heißt, anstatt der Mobilfunknummer werden Einweg-Pseudonyme genutzt. So kann der User bei selbem MCP jedes Mal mit unterschiedlichen Einweg-Pseudonymen einkaufen und bezahlen. Der MCP kann dann anhand der Einweg-Pseudonyme die wahre Identität des Users nicht erkennen.[574] Auf diese Weise kann der User eine partielle Anonymität durch Pseudonyme erreichen.[575]

Bei der Lieferung der physischen Produkte braucht der Händler die Anschrift bzw. Lieferadresse des Users nicht, da die Lieferung durch ein Lieferunternehmen erfolgt. Daher muss bei der Lieferung berücksichtigt werden, dass die Adresse nur an das Lieferunternehmen mitgeteilt wird. Zwar kennt das Lieferunternehmen die Identität des Users. Jedoch wird verhindert, dass diese personenbezogenen Daten wie der Name und die Adresse des Users in die Hände des Händlers kommen. Somit wird eine Möglichkeit der Verkettung der Lieferungen zu den Personen durch den Händler verhindert. Dies ist jedoch nicht unüberwindbar, da eine Kooperation zwischen dem Händler und dem Lieferunternehmen möglich ist, durch die beide Teilnehmer Daten und Informationen über den User tauschen können.[576] Mit dem vorgestellten Konzept

---

574 Vgl. mit den Erläuterungen im Abschnitt 4.4.2.3 Einweg-Pseudonyme, S. 105.

575 Vgl. mit den Erläuterungen im Abschnitt 4.4.2 Teilidentität - Pseudonymität - Partielle Anonymität, S. 102.

576 Vgl. Grimm/Lohndorf/Scholz (1999), S. 275; Enzmann/Eckert (2002), S. 10ff.

kann diese Möglichkeit für eine manipulative Kooperation erschwert werden. Das Lieferunternehmen bekommt die Lieferadresse der User, jedoch keine Kundennummer und keine Bankverbindung. Somit bleibt der User anonym.

7.3.3 Einrichtung eines Anonymitätsservices

Für die organisatorische Gestaltung eines anonymen Mobile Payment Systems, wie im Referenzprozessmodell dargestellt, ist die Einrichtung eines Anonymitätsservices entscheidend, da der mobile User erst durch die Nutzung dieses Anonymitätsservices anonyme Mobile Payments durchführen kann. Der Anonymitätsservice tritt zwischen dem mobilen User und seinen Transaktionspartnern als geheime Vermittlungsstelle auf. Das heißt, der MCP soll nicht erfahren, dass der User über einen Anonymitätsservice surft, einkauft und bezahlt. Bei einer Mobile Payment Transaktion werden die personenbezogenen Daten der mobilen User nicht bzw. anonymisiert übertragen.

Ein derartiger Service kann entweder als ein freiwilliger und unentgeltlicher Bürgerservice oder als ein Geschäftsmodell entwickelt und angeboten werden.[577] Einige Beispiele solcher Modelle gibt es schon im Internet wie der Anonymitätsservice AN.ON bzw. JAP.[578] Der Mobilfunkuser nutzt diesen Anonymitätsservice entgeltlich. Die Vorteile eines solchen Anonymitätsservices liegen auf der Hand. Danach kann ein solcher Anonymitätsservice für den User beispielsweise kostenpflichtig oder kostenfrei angeboten werden. Der User kann dann bei (Anonymitäts-)Bedarf den Service der Anonymisierung buchen und zahlen. Der Anonymitätsservice kann auf diese Weise Einnahmen aus der Anonymisierung bzw. Geheimhaltung der personenbezogenen Daten wie z. B. die IP-Nummer des Mobilfunkgerätes generieren und für eine schnelle Verbindung zwischen den Geschäftspartnern sorgen, sowie eine neue Kundenbasis schaffen.

Die Einrichtung eines Anonymitätsservices kann sowohl, als ein neues Geschäftsmodell, als auch durch die Mobilfunknetzbetreiber als Vermittlungs- bzw. Vertrauensstelle für anonyme Zahlungstransaktionen zwischen den mobilen Usern und MCP geschehen. Dadurch kann auch der Prozess der Zahlungstransaktionen vereinfacht

---

[577] Vgl. Seiffert (2006), S. 6ff.

[578] Die Praxisbeispiele für den Anonymitätsservice werden im Abschnitt 5.2.4 Anonymitätskonzepte S. 116ff. ausführlich erläutert. Vgl. auch http://anonymous-proxy-servers.net/de/, Stand: 05.02. 2010.

werden, etwa durch die Nutzung der eigenen internen Billing-Infrastruktur. Das heißt, der Mobilfunknetzbetreiber kann als eine Payment Mediation auftreten. Diese Payment Mediation ist eine Schnittstelle, die Komplexität der Verwendung der verschiedenen Zahlungsmethoden und Clearing-Kanäle für die verschiedenen MCP reduzieren kann. Wenn Mobilfunknetzbetreiber als Payment Mediation[579] auftreten, würden sie folgende Aufgaben übernehmen:[580]

- Mobilfunknetzbetreiber sammeln, managen und clearen Zahlungen durch eine Reihe von Zahlungsmöglichkeiten und -kanälen.
- MCP sind in der Lage, statische, dynamische, abonnement-basierte und sitzungsbasierte Preis-Modelle zu verwenden.
- Mobilfunknetzbetreiber können globalen Märkten Unterstützung für viele Währungen bieten.

Deshalb sind die Mobilfunknetzbetreiber (MNO), ebenso wie die Banken in einer besonderen und wichtigen Vertrauenspflicht. Die MNO haben großes Interesse, diese Kompetenz in ihren Händen zu halten und können neben der Rolle als Infrastrukturanbieter für die Telekommunikations- und Zahlungsdienste die Rolle einer TTP spielen. Für die Nutzung des Anonymitätsservices sollen jedoch Anreize geschaffen werden.

7.3.4 Einrichtung einer Trusted Third Party

Der konventionelle Ablauf eines Mobile Payment Systems kann mit der Beteiligung einer vertrauenswürdigen Instanz um eine TTP erweitert werden, um die Sicherheit und das Vertrauen im Zahlungssystem für alle Beteiligten zu schaffen.[581] Neben der Einsetzung eines Anonymitätsservices soll für die Gestaltung eines anonymen Mobile Payment Prozesses eine TTP eingesetzt werden, die für die Zertifizierung und Durchführung der Authentifizierung der Transaktionsparteien zuständig ist. Die TTP positioniert sich zwischen den Markteilnehmern im anonymen Mobile Payment

---

[579] Payment Mediation ist ein Vermittler zwischen User, Händler und Zahlungssystemen. Er ermöglicht Usern und Händlern über eine breite Basis verschiedener Zahlungsmöglichkeiten zu bezahlen bzw. abzurechnen. Vgl. Abrazhevich (2004), S. 29ff.

[580] Vgl. http://www.moremagic.com/solutions/payment_mediation.html, Stand: 05.02.2010.

[581] Die Trusted Third Parties werden im Abschnitt 3.1.7 Trusted Third Party, S. 60 ausführlich erläutert.

System. Demnach befindet sich die TTP zwischen dem mobilen User bzw. Anonymitätsservice und dem Händler bzw. MCP. In einem Mobile Payment System können die Mobilfunknetzbetreiber, Banken oder Kreditkartengesellschaften die Rolle einer TTP übernehmen, da sie ohnehin das Vertrauen von Transaktionsparteien genießen.[582] In diesem Zusammenhang können sich Mobilfunknetzbetreiber oder Banken und Kreditkartengesellschaften als TTP im Mobile Commerce positionieren und ein breites Servicespektrum anbieten.[583]

7.3.5 Unabhängigkeit des Anonymitätsservices und der Trusted Third Party

Die Vertrauensfrage und Unabhängigkeit des Anonymitätsservices sowie der TTP ist für die Gestaltung eines anonymen Mobile Payment Systems sehr wichtig. Beide Parteien gewinnen durch die Einrichtung eines Anonymitätsservices und der TTP eine strategische Position in der User-Authentifizierung bzw. User-Anonymität. Beide Services haben zwar die Möglichkeit User-Profile in Mobile Payment Prozessen zu erstellen bzw. diese offen zu legen. Jedoch dürfen sie diese Möglichkeit nur bei Betrugsfällen und Missbrauch auf die Forderung von und gegenüber den Behörden und Justiz zu nutzen.[584] Die Aufhebung der Anonymität erfolgt nur gegenüber den Justizbehörden für die Strafermittlung und -verfolgung.[585] Außerdem dürfen beide Services keine Zusammenarbeit weder miteinander noch mit anderen Prozessbeteiligten, vor allem mit den MCP bzw. Händlern eingehen. Aus geschilderten Gründen ist die Unabhängigkeit der beiden Parteien, des Anonymitätsservices und der TTP für die Funktion der User-Anonymität essenziell.[586] Deshalb soll die Unabhängigkeit der beiden Parteien bei der Gestaltung des anonymen Mobile Payment Prozesses gegeben sein oder möglichst durch die regulatorischen Maßnahmen gesichert werden. Beide Dienste sollen die Nutzung der Services und die Steigerung des Vertrauens in ihre Services durch eine sichere, bequeme und flexible Umgebung ermöglichen.

---

582 Vgl. Jain/Seri/Srinivasan (2008), S. 18; Khodawandi/Pousttchi/Wiedemann (2003), S. 53.

583 Vgl. Khodawandi/Pousttchi/Wiedemann (2003), S. 53.

584 Vgl. mit den Erläuterungen im Abschnitt 5.3.2 Strafrechtliche Aspekte der User-Anonymität, S. 148 sowie im Abschnitt 7.5.2 Berücksichtigung strafrechtlicher Aspekte, S. 201.

585 Vgl. mit den Erläuterungen im Abschnitt 5.3.2.2 Aufhebung und Aufdeckung der Anonymität des Users, S. 149.

586 Vgl. Seiffert (2006), S. 13.

7.3.6 Erforderliche Prozessanpassungen seitens der Markteilnehmer

Für die Realisierung der Grundidee, die im Abschnitt 7.3.1 Trennung der personenbezogenen Daten von den Transaktionsdaten, S. 179 dargestellt wurde, und die Gestaltung der User-Anonymität im anonymen Mobile Payment System sind einige Prozessanpassungen seitens der einzelnen Marktteilnehmer erforderlich. Deshalb sollen die erforderlichen Prozessanpassungen einzeln analysiert und erörtert werden. Dabei werden die Fragen beantwortet, beispielsweise, welcher Marktteilnehmer welche Daten benötigt, um Geschäftstransaktionen durchführen zu können. Welcher Marktteilnehmer soll welche Daten erhalten? Darüber hinaus soll unter der Berücksichtigung der Gesetzesgebote „Datensparsamkeit“ und „Datenvermeidung“ beantwortet werden, welche Daten der User zurückgehalten werden sollen bzw. können und wie dies ermöglicht werden kann? Die Analyse der Prozessanpassungen umfasst die folgenden Marktteilnehmer im anonymen Mobile Payment Prozess:

1. Prozessanpassungen und Ausstattung der User
2. Prozessanpassungen des Mobilfunknetzbetreibers
3. Prozessanpassungen des Anonymitätsservices
4. Prozessanpassungen des Mobile Content Providers
5. Prozessanpassungen der TTP
6. Prozessanpassungen der Bank
7. Prozessanpassungen der übrigen Prozessbeteiligten

In den folgenden Abschnitten sollen die hier aufgelisteten Prozessanpassungen seitens der Marktteilnehmer einzeln analysiert und erklärt werden:

7.3.6.1 Prozessanpassungen und Ausstattung der User

Im anonymen Mobile Payment System braucht sich der mobile User nicht zu registrieren, wenn er mobil bezahlen möchte. In der Regel ist das jedoch in vielen Mobile Payment Systemen der Fall. Das heißt, wenn der mobile User Mobile Payment nutzen möchte, muss der mobile User sich in Mobile Payment Systemen

registrieren.[587] Im dargestellten anonymen Mobile Payment System kann sich der User die Registrierungsphase im allgemeinen Mobile Payment System ersparen. Wenn der User anonyme Mobile Payments nutzen möchte, soll es ihm möglich sein, in einem ersten Szenario eine spezielle Applikation auf sein Mobilfunkgerät zu installieren, die er für die Anonymisierung braucht und kostenlos oder kostenpflichtig vom Anonymitätsservice bekommen kann.[588] In einem anderen Szenario soll es möglich sein, dass der User den Anonymitätsservice über einen Webservice des Anonymitätsserviceanbieters im WAP-Browser nutzen kann. Für die Nutzung des Services über das Web braucht er ein WAP-fähiges Mobilfunkgerät und einen installierten WAP-Browser.[589] Die meisten auf dem Markt befindlichen Mobilfunkgeräte sind moderne Multifunktionsgeräte und auch mit der WAP-Technologie ausgestattet.[590] Daher braucht der User unter diesen Bedingungen keine zusätzliche Hardware und Software für die Nutzung des Anonymitätsservices anzuschaffen. Wenn die technischen und regulatorischen Voraussetzungen für die Nutzung eines Anonymitätsservices vorliegen, kann der mobile User anonyme Mobile Payments durchführen. Es würden dabei keine Mobilfunknummer und Mobilfunkgerätenummer (IMEI) übermittelt. Die wahre mobile IP-Nummer soll bei der Anonymisierung durch die des Anonymitätsservices verschleiert werden. Neben diesen harten Faktoren gibt es bei den Prozessanpassungen auch weiche Faktoren, wie das Bewusstsein der User, ob er sich mit solchen Anonymitätsservices auskennt bzw. ob und wie er mit den harten Faktoren, also den notwendigen Prozessanpassungen und Ausstattungen umgehen kann. Hier könnte eine Hilfe für den User von den Prozessbeteiligten wie z. B. Anonymitätsservice und/oder Mobilfunknetzbetreiber selbst kommen und den Usern Informationen und Hilfe anbieten, z. B. wie man eine Anonymitätsapplikation auf das Mobilfunkgerät installieren und diese konfigurieren kann oder wie die Gesetzeslage für die Nutzung solcher Anonymitätsservices ist etc.

---

[587] Der Registrierungsprozess des User wird in einem allgemeinen Mobile Payment Prozess im Abschnitt 6.2 Analyse eines allgemeinen Mobile Payment Prozess, S. 154 ausführlich behandelt.

[588] Vgl. das Projekt AN.ON und JAP im Abschnitt 5.2.4.4 Mixe und deren Anwendung in der Praxis, S. 133ff und das Anonymitätsdienst TOR im Abschnitt 5.2.4.5 Onion Routing und dessen Anwendung in der Praxis, S. 138ff.

[589] Vgl. mit dem Abschnitt 5.2.4.1 Proxies und deren Anwendung in der Praxis, S. 125 und dem Abschnitt mCrowds und deren Anwendung in der Praxis, S. 132.

[590] Ausführliche Informationen finden sich im Abschnitt 2.6.1.2 WAP, S. 33.

7.3.6.2 Prozessanpassungen des Mobilfunknetzbetreibers

Die Mobilfunknetzbetreiber besitzen im Mobile Payment Prozess eine strategische Position, da sie eine technische Infrastruktur und gleichzeitig mobile Telekommunikationsdienste anbieten und eine breite Kundenbasis haben und damit einen Zugriff zu den personenbezogenen, Verbindungs- und Transaktionsdaten des mobilen Users haben.[591] Deshalb sollen diese Gegebenheiten der Mobilfunknetzbetreiber bei der Gestaltung eines anonymen Mobile Payment Systems berücksichtigt werden. Im anonymen Mobile Payment System braucht der Mobilfunknetzbetreiber zunächst keine großen Anpassungen vorzunehmen, da der mobile User wie bisher nur die Telekommunikationsdienste der Mobilfunknetzbetreiber nutzt und die anonymisierte Serviceanfrage des Users über den Anonymitätsservice erfolgt. Der Mobilfunknetzbetreiber erhält lediglich in der Billing-Phase eine Billing-Information, also eine Zahlungsforderung vom MCP, die im Zuge der anonymisierten Servicenutzung zustande kam. Darüber hinaus sendet der Mobilfunknetzbetreiber das Geld anonym an die Bank des MCP. Die personenbezogenen Daten sowie Transaktionsdaten sollen entsprechend dem aktuellen Datenschutzgesetzen und -richtlinien gespeichert und verwendet werden.[592]

7.3.6.3 Prozessanpassungen des Anonymitätsservices

Für die Gestaltung eines anonymen Mobile Payment Systems wurde bereits die Einrichtung einer neuen Instanz, nämlich eines Anonymitätsservices erläutert.[593] Diese neue Instanz im Mobile Payment System soll den mobilen Usern einen Anonymitätsservice anbieten. Der Anonymitätsservice hat die Aufgabe, die Identität des Users gegenüber den prozessbeteiligten Marktteilnehmern zu verheimlichen, indem z. B. dem MCP keine Serviceanfrage mit personenbezogenen Daten, sondern eine anonymisierte Serviceanfrage ohne personenbezogene Daten sendet. Der Anonymitätsservice positioniert sich im dargestellten Referenzprozessmodell zwischen dem mobilen User und MCP, darüber über die übrigen Marktteilnehmer hinaus. Damit der User den Anonymitätsservice nutzen kann, soll der Anonymitätsservice z. B. eine spezielle Anonymitätsapplikation oder einen WAP-Service für die Useranonymität

---

[591] Die Rolle und Interessen von Mobilfunknetzbetreiber werden im Abschnitt 3.1.3 Mobilfunknetzbetreiber, S. 58 ausführlich behandelt.

[592] Vgl. mit den Erläuterungen im Abschnitt 5.3.1 Gesetzliche Grundlagen zur User-Anonymität, S. 142 sowie im Abschnitt 7.5.1 Berücksichtigung gesetzlicher Rahmenbedingungen, S. 199.

[593] Vgl. mit den Erläuterungen im Abschnitt 7.3.3 Einrichtung eines Anonymitätsservices, S. 182.

anbieten.[594] Nur wenn der User anonym bleiben möchte, sendet er seine Serviceanfragen über den Anonymitätsservice. Wenn der Anonymitätsservice eine Serviceanfrage erhält, soll er diese in anonymisierter und verschlüsselter Form an den MCP und die TTP weiterleiten. Der MCP soll auf dieser Weise anonymisierte Serviceanfragen erhalten und keine Mobilfunknummer oder Mobilfunkgerätenummer des Users sehen. Stattdessen soll er die Mobile IP-Nummer des Anonymitätsservices erkennen. Mit der Anonymisierung soll dabei keine Partei im Mobile Payment Prozess benachteiligt werden, so dass sie ihre Geschäftprozesse entsprechend gestalten können.

7.3.6.4 Prozessanpassungen des Mobile Content Providers

Bei der Gestaltung eines anonymen Mobile Payment Systems soll der MCP seine Prozesse hinsichtlich der Anforderungen des Referenzprozessmodells anpassen. Bei anonymisierten Serviceanfragen vom mobilen User soll er nicht mehr die Identität des Users erkennen. Das heißt, er soll nicht mehr erfahren, wer bei ihm bestellt. Die Authentifizierung der User erfolgt über die TTP. Daher fragt er bei der TTP nach der Authentifizierung des Users nach, wenn er eine anonymisierte Serviceanfrage vom User bekommt. Wenn die Authentifizierung des Users erfolgreich ist, soll er dann die Lieferung des Services für den User autorisieren. Er kann dann die Nutzung des Services in Rechnung stellen und dies an den Mobilfunknetzbetreiber senden. Für die Bearbeitung einer anonymisierten Anfrage braucht der MCP mindestens ein Pseudonym des Users oder eine Sitzungs-ID[595] und den Namen des Mobilfunknetzbetreibers. Diese Mindestinformationen benötigt der MCP dafür, um erstens die Mobilfunknummer zu ermitteln, an die der Service geliefert werden soll und zweitens, um die korrekte Rechnungsstellung zu gewährleisten. MCP erkennt seine Kunden anhand eines Pseudonyms oder eine Sitzungs-ID, welche vom Anonymitätsservice vergeben werden, jedoch erkennt er den User hinter dem Pseudonym oder Sitzungs-ID nicht. MCP sendet die Rechnung mit dem Pseudonym oder Sitzungs-ID, dem Service und dem Betrag an den Mobilfunknetzbetreiber. Der User begleicht die Nutzung des Services, die er vom MCP erhalten hat, mit der Mobilfunkrechnung von seinem MNO. Der MCP stellt dafür die Nutzung des Services in Rechnung und schickt diese mit dem Pseudonym oder der Sitzungs-ID an den MNO. Der MNO

---

[594] Vgl. mit den Erläuterungen über die Nutzungsmöglichkeiten des Anonymitätsservices im Abschnitt 7.3.6.1 Prozessanpassungen und Ausstattung der User, S. 185.

[595] Vgl. mit der Fußnote 531, S. 157.

überweist das Geld an die Bank des MCP mit diesem Pseudonym oder dieser Sitzungs-ID.[596]

7.3.6.5 Prozessanpassungen der Trusted Third Party

Die TTP ist für die Bewahrung des öffentlichen Schlüssels und die Vergabe digitaler Signaturen der prozessbeteiligten Marktteilnehmer zuständig.[597] Daher soll die TTP den Authentifizierungsprozess des Users und anderer Parteien, wie im Referenzprozessmodell dargestellt, anpassen. Bei einer anonymisierten Serviceanfrage sendet der Anonymitätsservice die verschlüsselten Userdaten an die TTP. Beim Verschlüsselungsverfahren bleibt der private Schlüssel beim User. Der öffentliche Schlüssel wird an die TTP gesendet. Wenn die TTP vom MCP eine Anfrage der Authentifizierung des Users erhält, überprüft sie die Identität des Users und sendet eine Bestätigung, die die Echtheit der Useridentität beinhaltet, an den MCP zurück. Die TTP sendet jedoch in dieser Bestätigung keine personenbezogenen Daten.

7.3.6.6 Prozessanpassungen der Bank

Die Bank des MCP erhält die Überweisung bzw. Einzahlung des Geldes mit dem Pseudonym des Users oder der Sitzungs-ID. Der MCP gleicht dann bei seiner Bank die Einzahlungen mit den Pseudonymen oder Transaktionsnummern bzw. Sitzungs-IDs ab. Um die Zahlungsmodalitäten ordnungsgemäß auszuführen, benötigt die Bank folgende Daten: Einzahler, Bankverbindung, Höhe des Überweisungsbetrages und Verwendungszweck der Zahlung. Beim Verwendungszweck soll eine Transaktionsnummer in Form des User-Pseudonyms oder der Sitzungs-ID angegeben werden, mit der der MCP in der Lage ist, diese Zahlung der entsprechenden Leistung zu zuordnen.

7.3.6.7 Prozessanpassungen der übrigen prozessbeteiligten Marktteilnehmern

Bei der Gestaltung eines anonymen Mobile Payment Systems sollen die prozessbeteiligten Marktteilnehmer ihre Geschäftsprozesse anpassen. Für die Realisierung

---

[596] Vgl. mit den Erläuterungen im Abschnitt 7.3.6.6 Prozessanpassungen der Bank, S. 189.

[597] Vgl. Fox/Horster/Kraaibeek (1995), S. 4ff. sowie mit dem Abschnitt 3.1.7 Trusted Third Party, S. 60.

eines anonymen Mobile Payment Systems sind spezielle Hard- und Software erforderlich. Beispielsweise auf der Userseite benötigt der User moderne Mobilfunkgeräte mit WAP-Technologie. Außerdem ist es erforderlich, Usern Identity Management Applikation anzubieten, damit sie ihre Identität bzw. Anonymität in verschiedenen Kauf- und Zahlungssituationen selbst bestimmen können. Daher sollen sowohl die Gerätehersteller als auch Softwarehersteller die Anforderungen der User bzw. des anonymen Mobile Payment Systems berücksichtigen und entsprechende mobilen Technologien und Produkte anbieten. Der Staat soll seiner Aufsichtfunktion bei der Gestaltung der anonymen Mobile Payment Systeme nachkommen. Dabei soll er u. a. die Gesetzeskonformität und -verstöße der einzelnen Marktteilnehmer bei den anonymen Mobile Payment Systemen und Transaktionen kontrollieren.

Zusammenfassend kann festgehalten werden, dass ein reibungsloses Funktionieren eines anonymen Mobile Payment Systems im Referenzprozessmodell in erster Linie von den organisatorischen Gestaltungsmöglichkeiten abhängig ist. Erst wenn die Marktteilnehmer entsprechende Anpassungen in ihren Geschäftsprozessen, wie dies bereits gezeigt wurde, vornehmen, kann ein anonymes Mobile Payment System zustande gebracht werden, das den Anforderungen der Marktteilnehmer, vor allem des Users, entspricht. Der Kundennutzen mit der Erfüllung der User-Anonymität hat enorme Wirkung auf das Vertrauen des Users an Mobile Payment Systeme in Zeiten der Vorratsdatenspeicherung, des Datenklau und der Datenmanipulation.

7.4 Technische Gestaltungsmöglichkeiten

Bei der Gestaltung eines anonymen Mobile Payment Systems sollen die technischen Rahmenbedingungen und Möglichkeiten berücksichtigt werden.[598] Insbesondere bieten hier die Anonymitätskonzepte für die Gestaltung eines anonymen Mobile Payment Systems eine interessante Grundlage. Die erfolgreichen Beispiele, die sich in der Praxis der User-Anonymität im Internet bewährt haben, können auch für die User-Anonymität in Mobile Payment Systemen und Anwendungen eingesetzt werden.[599] Wie diese technischen Gestaltungsmöglichkeiten verwendet werden können, werden in folgenden Abschnitten erläutert. Hierbei umfasst die technische

[598] Die technischen Rahmenbedingungen der Anonymität werden im Abschnitt 5.2 Technische Rahmenbedingungen der Anonymität, S. 122 ausführlich behandelt.

[599] Die Anonymitätskonzepte und -techniken werden im Abschnitt 5.2.4 Anonymitätskonzepte, S. 124ff. ausführlich behandelt.

Gestaltung des im Referenzprozessmodell dargestellten anonymen Mobile Payment Systems die folgenden technischen Gestaltungsmöglichkeiten:

- technische Gestaltung eines Anonymitätsservices
- Bewertung der Eignung und Übertragbarkeit der Anonymitätskonzepte
- Berücksichtigung digitaler Verschlüsselungstechniken und Signaturen
- Verschlüsselung der personenbezogenen Daten und Transaktionsdaten
- Berücksichtigung der Funktion von Trusted Third Parties und Certification Authorities

7.4.1 Technische Gestaltung eines Anonymitätsservices

Für die Gestaltung eines Anonymitätsservices sollen die vorhandenen Anonymitätstechniken und deren Anwendungen in der Praxis berücksichtigt werden. Durch neue Anonymisierungsdienste können z. B. neue Geschäftsmodelle kreiert werden.[600] Um die technische Gestaltung eines Anonymitätsservices zu ermöglichen, sollen die Eignung und Übertragbarkeit der Anonymitätskonzepte einzeln bewertet werden, die in den folgenden Abschnitten erläutert werden.

7.4.2 Eignung und Übertragbarkeit der Anonymitätskonzepte

Wie bereits erläutert wurde, bieten die Anonymitätskonzepte vielfältige Möglichkeiten zur Gestaltung der User-Anonymität.[601] Diese Konzepte werden in der Praxis für die User-Anonymität im Internet erfolgreich angewendet.[602] Diese Konzepte können auch für die Gestaltung der User-Anonymität in Mobile Payment Systemen angewendet werden. Für diesen Zweck sollen diese Anonymitätskonzepte weiter entwickelt und in der Praxis der Mobile Payment Systeme erprobt werden. Daher sollen im Folgenden die Eignung und Übertragbarkeit dieser Konzepte für die Gestaltung anonymer Mobile Payment Prozesse und Systeme analysiert und bewertet werden. Die Analyse und Bewertung der Eignung und Übertragbarkeit soll nach den folgenden Kriterien bzw. Fragen erfolgen:

---

600 Vgl. Seiffert (2006), S. 6ff.; Heuer/Ulmer (2006), S. 7ff.

601 Vgl. mit den Erläuterungen im Abschnitt 5.2.4 Anonymitätskonzepte, S. 124ff.

602 Vgl. Ebenda.

- Welche Erfahrungswerte liegen im Bereich Mobile Payment und anderen Feldern vor?
- Welche Performanz ist bei Mobile Payment, bei der User-Anonymität zu erwarten?
- Welchen Schutz können die einzelnen Konzepte gegen die vorhandenen und potentiellen Angriffe, Risiken und Gefahren bieten?
- Welche technische Spezifikation ist für das organisatorische Konzept erforderlich?
- Sind die einzelnen Konzepte voll oder partiell übertragbar?
- Welche Einschränkungen sind den einzelnen Konzepten ausgesetzt?
- Sind die einzelnen Konzepte erweiterbar oder sogar um- oder nachrüstbar?
- Können die einzelnen Konzepte die gesetzlichen Kriterien und Regeln erfüllen?

Alle hier aufgelisteten Fragen und Kriterien bedürfen einer Klärung der Möglichkeiten und Voraussetzungen für eine Übertragbarkeit auf die User-Anonymität in Mobile Payment Systemen. Deshalb sollen im Folgenden die einzelnen Anonymitätskonzepte im Lichte der aufgelisteten Kriterien und Fragen analysiert und bewertet werden.

7.4.2.1 Eignung und Übertragbarkeit des Anonymitätskonzeptes Proxies

Das Konzept der Proxies kann unter Umständen für die User-Anonymität in Mobile Payment Systemen eingesetzt werden. Wie bereits erklärt wurde, wird der Proxy zwischen dem User-Rechner und den Rechnern bzw. Servern von anderen Marktteilnehmern eingesetzt.[603] Das Konzept der Proxies wird im Internet für die Anonymisierungsdienste benutzt, um die eigene IP-Adresse zu verschleiern und im Internet anonym surfen zu können. Die anonymen Proxies werden im stationären Internet von einigen Anonymisierungsdiensten kostenfrei oder –pflichtig angeboten. Analog zu diesem Prinzip kann ein mobiler User einen Proxy in der Mobile-Umgebung nutzen, der die Anonymität des mobilen Users gewährleistet. Ein solcher Anonymitätsservice kann in der mobilen Umgebung für Mobile Commerce und

[603] Das Konzept der Proxies wird im Abschnitt 5.2.4.1 Proxies und deren Anwendung in der Praxis, S. 125 ausführlich behandelt.

Payment von (neuen) Anonymisierungsdiensten kostenfrei oder kostenpflichtig angeboten werden.

Wenn der mobile User mit seinem Mobilfunkgerät im Internet mit einem WAP-Browser surfen und dabei anonym bleiben möchte, kann er die Anonymisierungsdienste nutzen. Wenn der mobile User z. B. ein digitales Produkt oder einen digitalen Service kauft, muss er sich in der Regel beim MCP registrieren und seine personenbezogenen Daten wie z. B. Mobilfunknummer angeben. Wenn aber der User über einen Proxy in der mobilen Umgebung surft, ein digitales Produkt kaufen bzw. bezahlen und dabei anonym bleiben möchte, kann er zwar seine mobile IP-Nummer und seinen Internet Provider verschleiern, jedoch ist seine Mobilfunknummer für die Lieferung des Produktes nötig, da der MCP das gewünschte Produkt an diese Nummer liefert. Die Frage ist dabei, wie der User das gewünschte Produkt anonym kaufen und bezahlen kann, ohne zusätzlich seine Mobilfunknummer an den MCP zu übertragen. Eine Möglichkeit zur Beantwortung wäre die Nutzung der Pseudonyme, beispielsweise der Einweg-Pseudonyme zusätzlich zur Nutzung der Proxy-Technik.[604] Mit der Einsetzung und Nutzung der Kombination beider Lösungsansätze kann ein bestimmter Grad an User-Anonymität, nämlich eine partielle Anonymität erreicht werden.

Die Nutzung des Proxy-Konzeptes kann für die Anwender Kostenvorteile bringen, da die Anwendung dieses Konzeptes keinen großen Aufwand erfordert. Außerdem können die Proxies kürzere Antwortzeiten in der mobilen Umgebung bieten. Allerdings könnte diese Geschwindigkeit in der mobilen Umgebung nicht immer gegeben sein. Bei einer Nutzung des Proxy-Konzeptes werden zwar die Daten der Serviceanfragen verschlüsselt übertragen. Die Inhalte der Serviceanfragen können nicht von Angreifern oder Beobachtern gesehen werden. Jedoch können die Länge und die Zeit der Serviceanfragen verkettet werden. Ein Angreifer oder Beobachter in der mobilen Umgebung kann die Daten verketten und Verkehrsanalysen durchführen. Daher bietet diese Anonymisierungstechnik wenig Schutz vor Angriffen und keine absolute Anonymität für die User. Aber es ist der einfachste Weg, eine schnelle Basis-Anonymität für den User herzustellen. Um auch eine solche Möglichkeit bieten zu können, müssen die organisatorischen und technischen Rahmenbedingungen bei den Marktteilnehmern erschaffen werden.

---

[604] Die Lösungsansätze und Nutzung der Pseudonyme werden im Abschnitt 4.4.2 Teilidentität - Pseudonymität - Partielle Anonymität, S. 102 ausführlich erklärt.

Beispielsweise können die Mobilfunknetzbetreiber neben ihrer traditionellen Rolle als eine TTP auftreten. Diese TTP kann die personenbezogenen und Verbindungsdaten der User zurückhalten und nicht an die Online-Händler und Content Provider weitergeben. Beim Einsatz eines Proxy kann der Content Provider nicht die WAP-Adresse und Geräte-Adresse des Users sehen. Er kann nur die Proxy-Adresse des Anonymitätsservices sehen, nicht aber den User, der den Anonymitätsservice in Anspruch nimmt. Hierfür muss die Möglichkeit gegeben werden, dass der User seine WAP-Browser konfigurieren und anonyme Server des Anonymitätsservices manuell oder automatisch wählen kann. Des Weiteren hat der mobile User die Möglichkeit, über die webbasierten Anonymisierungsdiensten zu surfen und zu bezahlen.

7.4.2.2 Eignung und Übertragbarkeit der Anonymitätskonzepte Crowds und mCrowds

Wie bereits erläutert wurde, bieten das Anonymitätskonzept Crowds und seine Erweiterung mCrowds eine interessante und hilfreiche User-Anonymität in mobilen Umgebungen.[605] Nach dem Konzept von Crowds bzw. mCrowds kann anonymes Surfen mit WAP-fähigen Mobilfunkgeräten gewährleistet werden. mCrowds kann beispielsweise bei Location based services eingesetzt werden, damit eine Weitergabe von personenbezogenen Daten und Informationen an den MCP minimiert werden kann. Daher kann mCrowds unter gegebenen Voraussetzungen für die Gestaltung der User-Anonymität in Mobile Payment Systemen eingesetzt werden. Auf diese Weise kann eine bestimmte Client-Anonymität und Ort-Anonymität erreicht werden.

Um die mCrowds zu benutzen, soll der mobile User die mCrowds-Applikation auf seinem Mobilfunkgerät installieren und nach der Installation diese konfigurieren. Der User kann dann über einen WAP-Browser anonym im Internet surfen. Wenn er im Internet ein digitales Produkt kauft, muss er nicht seine personenbezogenen Daten an den Content Provider oder Online-Händler preisgeben. Für die mCrowds-Applikation wird ein plattformunabhängiger WAP-Proxy benutzt, der eine Schnittstelle für die vertraulichen personenbezogenen Daten und Informationen ist. Die mCrowds-Applikation und WAP-Proxy soll unter Kontrolle der mobilen User oder einer Trusted Third Party sein. Da das Konzept von mCrowds in der Praxis bisher nicht erprobt wurde, besteht das Konzept mCrowds als eine theoretische Möglichkeit für die Gestaltung der User-Anonymität in Mobile Payment Systemen, dessen Performanz erst

[605] Die Anonymitätskonzepte Crowds und mCrowds werden im Abschnitt 5.2.4.2 Crowds und deren Anwendung in der Praxis, S. 129 und im Abschnitt 5.2.4.3 mCrowds und deren Anwendung in der Praxis, S. 132 ausführlich erläutert.

nach den ersten Erfahrungen in der Praxis von Mobile Payment Systemen bewertet werden kann.

7.4.2.3 Eignung und Übertragbarkeit des Anonymitätskonzeptes Mix-Netze

Eine weitere Möglichkeit für die Gestaltung der User-Anonymität in Mobile Payment Systemen ist das Konzept der Mixe-Netze. Das Konzept der Mix-Netze bietet den Usern eine Client-Anonymität und Kommunikationsanonymität.[606] Für die anonyme Internetnutzung über die Mix-Netze wurden verschiedene Anonymisierungsdienste entwickelt und werden in der Praxis von den Usern benutzt. Eine dieser Anonymisierungsdienste ist das JAP-Projekt, das sehr bekannt ist und von den meisten Usern benutzt wird.[607] Für die Gestaltung der User-Anonymität in Mobile Payment Systemen kann das Konzept der Mixe angewendet und dies für mobile Anwendungen in mobiler Umgebung erweitert werden. Dafür kann eine spezielle Proxy-Server-Applikation für Clients, also mobile User ähnlich wie bzw. auf der Basis der JAP-Applikation entwickelt werden. In einem Anonymisierungsdienst kann dann diese Applikation den mobilen Usern angeboten werden. Die User können dann eine Möglichkeit zum Selbstschutz gegen professionelle Datensammler erhalten. Auf diese Weise kann eine bestimmte Client-Anonymität und Ort-Anonymität erreicht werden. Die Anonymisierungsdienste bzw. die Betreiber der Mix-Netze sollen Vertrauen bei den mobilen Usern bilden, indem sie nicht mit den anderen Marktteilnehmern wie z. B. mit den Händlern zusammenarbeiten. Der Anonymisierungsdienst JAP zeigt jedoch einige Schwächen, wenn ein Angreifer das gesamte Netzwerk überwacht.[608] Gegen den Angreifer, der das gesamte Internet überwacht oder den ersten und letzten Mix kontrolliert, kann das System noch nicht schützen. Außerdem darf ein Mix der Kaskade nicht vom Angreifer kontrolliert werden und nicht mit dem Angreifer zusammenarbeiten.[609]

---

606 Das Konzept der Mix-Netze wird im Abschnitt 5.2.4.4 Mixe und deren Anwendung in der Praxis, S. 133 ausführlich behandelt.

607 Das Konzept der Mix-Netze wird im Abschnitt 5.2.4.4 Mixe und deren Anwendung in der Praxis, S. 133 ausführlich behandelt.

608 Vgl. mit den Erläuterungen und Beispiele im Abschnitt 5.2.4.4 Mixe und deren Anwendung in der Praxis, S. 133.

609 Vgl. Ebenda.

7.4.2.4 Eignung und Übertragbarkeit des Anonymitätskonzeptes Onion Routing

Eine andere Möglichkeit für die Gestaltung der User-Anonymität in Mobile Payment Systemen besteht mit dem Konzept des Onion Routings, das eine private anonyme Kommunikation über die öffentlichen Netzwerke durch eine Zahl von Knotenpunkte, den „onion routers“, ermöglicht wird. Danach werden die Nachrichten unter den Endusern als verschlüsselte „data onions“ durch einen zufälligen Pfad von vermittelnden Onion Routers gesendet. Ein bekanntes Beispiel ist der Anonymisierungsdienst mit dem TOR-Projekt.[610] Auf der Basis der TOR-Software kann beispielsweise eine spezielle Applikation entwickelt werden. Nach dem Prinzip der TOR-Software kann die neue Applikation eine verschlüsselte Verbindung mit einem der im Netzwerk verfügbaren Server aufbauen. Die Verbindung kann in mobiler Umgebung zwiebelartig verschlüsselt werden. Danach wird die Verbindung schrittweise über die zufällig gewählte Route erweitert und ein Kreis gebildet. Jeder Knoten kennt entlang der Route nur, wer Vorgänger-Knoten war und Nachfolger-Knoten ist. Kein Knoten kennt jemals die gesamte Route.

Für eine Route werden jeweils drei Server (Knoten) ausgewählt, um eine minimale Anonymität zu erreichen. Jede Route dauert eine Minute. Danach wechselt sich die Route. Die Nachrichten werden zwiebelartig verschlüsselt. Auch wenn zwei Knoten einer Route korrumpiert wurden oder mindestens ein Knoten vertrauenswürdig bleibt, kann ein Angreifer oder Beobachter die Nachrichten nicht mitlesen. Dadurch wird die Anonymisierung der Kommunikation gewährleistet. Der Ziel-Webserver kann nur die IP-Adresse des letzten TOR-Knotens der Route sehen. Der ursprüngliche User bleibt somit anonym.

Derzeit besteht das TOR-Netzwerk aus ca. 2000 Servern (Knoten), die weltweit verteilt sind. Ein Onion Router kann auch für andere Anwendungen, beispielsweise für Instant Messaging, IRC, SSH, E-Mail, P2P etc. genutzt werden, da ein Onion Router ein Socks Proxy ist. Dabei bietet TOR auch sogenannte Hidden Services (Versteckte Dienste), um die Aufenthaltsorte von Usern (Ortanonymität) zu verbergen. Außerdem können andere TOR-User sogenannte TOR "Rendezvouspunkte" verwenden, um

---

[610] Vgl. mit den Erläuterungen und Beispiele im Abschnitt 5.2.4.5 Onion Routing und dessen Anwendung in der Praxis, S. 138.

Hidden Services zu nutzen, ohne dabei die Netzwerkidentität des Anderen zu kennen.[611]

7.4.3 Berücksichtigung digitaler Verschlüsselungstechniken und Signaturen

Wie bereits erwähnt können digitale Verschlüsselungstechniken für die Gestaltung der User-Anonymität in Mobile Payment Systemen eingesetzt werden, um eine bestimmte Kommunikationsanonymität und Sicherheit zu erreichen bzw. zu gewährleisten. Im Referenzprozessmodell wurde die asymmetrische Verschlüsselungstechnik angewandt. Die Verschlüsselungstechniken helfen, die Inhalte der Daten vor unberechtigten Personen und Institutionen zu schützen. Bei der symmetrischen Verschlüsselung wird der gleiche Schlüssel für die Codierung (Verschlüsselung) und Decodierung (Entschlüsselung) einer Nachricht verwendet. Bei einer Kommunikation kennen die beteiligten Transaktionspartner den Schlüssel, z. B. DES.[612] Bei der asymmetrischen Verschlüsselung hingegen werden zwei verschiedene Schlüssel für die Codierung und Decodierung verwendet. Jeder Transaktionspartner besitzt zwei Schlüssel, nämlich einen privaten und einen öffentlichen Schlüssel, z. B. RSA.[613] Daher können die beiden Verschlüsselungstechniken (symmetrische und asymmetrische Verfahren) einzeln oder in Kombination für die Inhalte der Serviceanfragen und Zahlungstransaktionen eingesetzt werden. Zusätzlich können digitale Signaturen mit privaten und öffentlichen Schlüsseln genutzt werden.[614]

---

611 Vgl. mit den Erläuterungen im Abschnitt 5.2.4.5 Onion Routing und dessen Anwendung in der Praxis, S. 138 und http://www.torproject.org/overview.html.de sowie http://wiki.privacyfoundation.de/TOR%20Onion%20Router, Stand: 07.01.2009.

612 DES, Der Data Encryption Standard ist ein symmetrisches Verschlüsselungsverfahren. Die von einer dritten Partei zu schützenden Daten werden vom Absender mit einem geheimen Schlüssel chiffriert. Nach der Übertragung der chiffrierten Daten über das Internet werden die empfangenen Daten vom Empfänger mit dem gleichen Schlüssel, mit dem die Nachricht verschlüsselt wurde, wieder entschlüsselt. Um eine Informationsübertragung zwischen Absender und Empfänger zu realisieren, muss vorher der Schlüssel möglichst persönlich bzw. über eine entsprechend gesicherte Kommunikationsverbindung ausgetauscht werden. Vgl. Meißner (2002), S. 4.

613 Vgl. mit den Erläuterungen über das RSA-Verfahren in der Fußnote 354, S. 96.

614 Vgl. mit den Erläuterungen im Abschnitt 3.1.7 Trusted Third Party, S. 60.

7.4.3.1 Verschlüsselung der personenbezogenen Daten und Transaktionsdaten

Bei der Gestaltung der User-Anonymität in Mobile Payment Systemen soll berücksichtigt werden, dass die personenbezogenen Daten und Transaktionsdaten verschlüsselt werden. Diese Verschlüsselung der personenbezogenen Daten und Transaktionsdaten können, wie im vorigen Abschnitt bereits erläutert wurde, durch die Nutzung der asymmetrischen Verschlüsselungstechnik durchgeführt werden. Auf diese Weise können die Inhalte dieser Daten von Angreifern und Beobachtern nicht gelesen werden. Dies ermöglicht eine bestimmte Kommunikationsanonymität unter den Prozessbeteiligten. Darüber hinaus sollen die digitalen Zertifikate zur gegenseitigen Authentifizierung der User und anderen Prozessbeteiligten genutzt werden. Daher sollen auch die Trusted Third Parties oder Certification Authorities für die Beglaubigung der Identitäten berücksichtigt werden. Im Folgenden sollen die beiden Bereiche erläutert werden.

7.4.3.2 Berücksichtigung der Funktion von Trusted Third Parties und Certification Authorities

Für die Gestaltung der User-Anonymität in Mobile Payment Systemen spielen die Trusted Third Parties, auch als Trust Center oder Certificate Authorities bekannt, eine wichtige Rolle, da sie mit den digitalen Zertifikaten die Identität von Usern und Datenanbietern oder anderen Transaktionspartnern beglaubigen. Diese Zertifikate fungieren als digitale Ausweise für die User.[615] Daher soll die Funktion der Trusted Third Parties bei der Gestaltung der User-Anonymität berücksichtigt werden.[616]

Zusammenfassend kann festgehalten werden, dass das reibungslose Funktionieren eines anonymen Mobile Payment Systems u. a. von den technischen Gestaltungsmöglichkeiten abhängig ist. Die Anonymitätskonzepte geben hier eine gute Basis für die technische Gestaltung eines anonymen Mobile Payment Systems. Die einzelnen Beispiele der einzelnen Anonymitätskonzepte verdeutlichen diese technischen Gestaltungsmöglichkeiten. Deshalb sollen sie schon im Vorfeld der Konzept- oder Designphase der anonymen Mobile Payment Systeme berücksichtigt werden, wenn

---

[615] Die Rolle von Trusted Third Parties wird im Abschnitt 3.1.7 Trusted Third Party, S. 60 ausführlich behandelt.

[616] Die Rolle und Funktion der Trusted Third Party im anonymen Mobile Payment im Abschnitt 6.4.1 Beschreibung des anonymen Mobile Payment Prozesses, S. 161.

ein Kundennutzen mit der User-Anonymität beabsichtigt wird. Die Erfahrungen der User mit den Mobile Payment Systemen sowie deren Anforderungen sollen schon im Vorfeld der Konzept- oder Designphase quantifiziert, gemessen und in die technischen Spezifikationen umgesetzt werden.

7.5 Regulatorische Gestaltungsmöglichkeiten

Wie bereits erläutert wurde, bestimmen die regulatorischen Rahmenbedingungen die Verhältnisse der User und Serviceprovider sowie der anderen Marktteilnehmer. Sie sollen bei der Gestaltung der User-Anonymität in Mobile Payment Systemen berücksichtigt werden.[617] Hierfür sollen die gesetzlichen Grundlagen und strafrechtlichen Aspekte der User-Anonymität berücksichtigt werden, die im Folgenden näher erklärt werden.

7.5.1 Berücksichtigung gesetzlicher Rahmenbedingungen

Bei der Gestaltung eines anonymen Mobile Payment Systems sollen die gesetzlichen Rahmenbedingungen zur User-Anonymität berücksichtigt werden.[618] Folglich sollen die Prozessbeteiligten in anonymen Mobile Payment Systemen nach den geltenden Datenschutzbestimmungen handeln. Insbesondere die gesetzlichen Datenschutzbestimmungen wie das Verbotprinzip mit Erlaubnisvorbehalt, Datenvermeidung und Datensparsamkeit spielen eine wichtige Rolle. Bei der Bestimmung des Verbotsprinzips mit Erlaubnisvorbehalt dürfen die Prozessbeteiligten die personenbezogenen Daten im Mobile Payment System nur mit ausdrücklicher gesetzlicher Erlaubnis oder mit Zustimmung der Person, um deren Daten es geht, erheben, verarbeiten und nutzen. Danach sollen der MCP und andere Beteiligte die personenbezogenen Daten der User sowie deren Mobile Payment-Transaktionsdaten erst mit der Zustimmung der betroffenen Person erheben, verarbeiten und nutzen dürfen. Bei dem Grundsatz der Datenvermeidung und Datensparsamkeit sollen die Prozessbeteiligten ihre Geschäftsprozesse im anonymen Mobile Payment System so ausrichten, dass sie keine oder möglichst wenige personenbezogenen Daten der User bei den Mobile Payment Transaktionen verwenden müssen.

---

617 Die regulatorischen Rahmenbedingungen der Anonymität werden im Abschnitt 5.3 Regulatorische Rahmenbedingungen der Anonymität, S. 140 ausführlich behandelt.

618 Die gesetzlichen Rahmenbedingungen der Anonymität werden im Abschnitt 5.3.1 Gesetzliche Grundlagen zur User-Anonymität, S. 142 ausführlich behandelt.

Konkretisiert werden diese Datenschutzbestimmungen in den EU-Richtlinien sowie den Gesetzen und Verordnungen in Deutschland. § 3a BDSG betont die Gestaltung der Datenverarbeitungssysteme und Nutzung der Möglichkeiten der Anonymisierung und Pseudonymisierung mit dem Umgang personenbezogener Daten. Danach sollen die Möglichkeiten der Anonymisierung und Pseudonymisierung bei der Gestaltung der User-Anonymität in Mobile Payment Systemen genutzt werden. In den §§ 29 und 30 BDSG wird das geschäftsmäßige Erheben, Speichern oder Verändern personenbezogener Daten zum Zweck der Übermittlung in anonymisierter Form geregelt. Danach sollen die personenbezogenen Daten, die in den Mobile Payment Transaktionen geschäftsmäßig erhoben und gespeichert werden, in anonymisierter Form übermittelt werden. Die Merkmale, mit denen Einzelangaben über persönliche und sachliche Verhältnisse einer Person zugeordnet werden können, sollen gesondert gespeichert werden. Die gesonderte bzw. anonyme Speicherung der Daten wurde bereits in der Trennung der personenbezogenen Daten von den Transaktionsdaten erklärt.[619]

Neben dem BDSG sollen die jeweiligen Gesetze im TKG bei der Gestaltung der User-Anonymität in Mobile Payment Systemen berücksichtigt werden. In den §§ 88-115 TKG sind die Schutzverpflichtungen der Netzbetreiber sowie deren Informationspflichten gegenüber dem Kunden, der Schutz personenbezogener Kundendaten, geregelt. Im § 96 TKG ist der Umgang mit den Verkehrsdaten von Kunden geregelt. § 98 TKG regelt die Verwendung von Standortdaten von Kunden. Auch in diesen Paragrafen werden die Anonymisierung der Daten der Kunden und die Einwilligung der Teilnehmer betont. Daher sollen die Prozessbeteiligten diese Gesetze bei der Gestaltung der Anonymität berücksichtigen.

Außer dem TKG sollen die jeweiligen Gesetze im TMG bei der Gestaltung der User-Anonymität in Mobile Payment Systemen berücksichtigt werden. In den Paragrafen §§ 13-15 TMG werden die Möglichkeit der Nutzung durch Anonymität und Pseudonymität, die Erhebung und Verwendung von Bestands- und Nutzungsdaten sowie die Erstellung von Nutzungsprofilen durch die Möglichkeit der Nutzung von Pseudonymen erwähnt. Daher sollen die Prozessbeteiligten diese Gesetze bei der Gestaltung der Anonymität berücksichtigen.

---

[619] Vgl. mit den Erläuterungen im Abschnitt 7.3.1 Trennung der personenbezogenen Daten von den Transaktionsdaten, S. 179 sowie mit den Erläuterungen über die Datenschutzanforderungen im Abschnitt 3.2.2.2 Integrations- und Realisierungsanforderungen, S. 68.

Neben den Gesetzen und Verordnungen in Deutschland gibt es Regelungen und Richtlinien auf der EU-Ebene wie z. B. die EU-Datenschutzrichtlinie 95/46/EG, die in Deutschland mit dem Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze in nationales Recht umgesetzt wurde. Außerdem regelt die Europäische Datenschutzkonvention die Rechte und Grundfreiheiten der Vertragsparteien und erwähnt insbesondere die Achtung der grundlegenden Persönlichkeitsrechte beim freien, grenzüberschreitenden Informationsaustausch und Schutz personenbezogener Daten, die automatisiert verarbeitet werden.[620] Daher sollen die Prozessbeteiligten diese Gesetze bei der Gestaltung der Anonymität berücksichtigen.

Neben der Berücksichtigung der gesetzlichen Rahmenbedingungen sollen neue gesetzliche Regelungen für die Gestaltung der User-Anonymität geschaffen werden, da veränderte oder neu geschaffene Mobile Payment Systeme dies erfordern. Im dargestellten Referenzprozessmodell wurde von einem neuen Anonymitätsservice ausgegangen, der die User-Anonymität gewährleistet. Die Nutzung eines solchen Anonymitätsservice soll unter Umständen gesetzlich untermauert werden.

7.5.2 Berücksichtigung strafrechtlicher Aspekte

Wie bereits erläutert wurde, kann es auch in einem anonymen Mobile Payment System zur Manipulation und Missbrauch kommen.[621] Bei der Gestaltung eines anonymen Mobile Payment Prozesses sollen die strafrechtlichen Aspekte berücksichtigt werden.

Bei der Gestaltung eines anonymen Mobile Payment Systems soll berücksichtigt werden, dass eine Aufdeckung bzw. Aufhebung der User-Anonymität bei Betrugs-, Missbrauchs- und Manipulationsfällen möglich ist. Da ein Anonymitätsservice alle Zugriffe eines Users mit einer Kooperation seiner Systemmitglieder herausfinden kann und somit eine rückverfolgbare Anonymität möglich ist, soll beachtet werden, dass die Aufdeckung und Aufhebung der User-Anonymität nur unter strengen Auflagen erfolgen darf. Gleichzeitig soll diese Möglichkeit der Aufdeckung und Auf-

---

620 Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten. Vgl. http://conventions.coe.int/Treaty/GER/Treaties/Html/108.htm, Stand: 12.07. 2009.

621 Die strafrechtlichen Aspekte der Anonymität werden im Abschnitt 5.3.2 Strafrechtliche Aspekte der User-Anonymität, S. 148 ausführlich behandelt.

hebung jedoch nicht als eine Überwachung des Users in seinen Mobil Payment Aktivitäten interpretiert bzw. implementiert werden.

Dies hängt auch mit der Vorratsdatenspeicherung und Überwachung der Netzwerke zusammen.[622] Der Gesetzgeber zwang den Service Provider bis zum Urteil vom 02.03.2010 durch das Bundesverfassungsgericht dazu, alle Kommunikationsvorgänge zu protokollieren und mindestens sechs Monate zu speichern.[623] Nach diesem Urteil sollen Service Provider nicht mehr Daten speichern sowie alle bisher unter den Regeln gespeicherten Daten unverzüglich löschen, da die Vorratsdatenspeicherung verfassungswidrig ist. So wird es nicht mehr möglich sein, alle Daten zu speichern, die in Mobile Payment Transaktionen auftauchen, auch wenn sie anonym durchgeführt wurden. Jedoch ist eine Vorratsdatenspeicherung generell nicht auszuschließen. Das heißt, bei Straf- oder Verdachtfällen ist eine Vorratsdatenspeicherung nur unter strengen Regeln zulässig. Eine Deanonymisierung darf nur für die Zwecke der Strafverfolgung unter strengen Auflagen möglich sein. Jedoch soll dies nicht zur Überwachung der Dienste und der User erweitert werden.

Für die Verfolgung und Aufklärung der Straftaten mittels Telekommunikation besteht ein Anspruch, die Herausgabe der Verkehrsdaten nach § 100g StPO, § 113a TKG und in § 113b TKG. Ebenso besteht Anspruch auf Herausgabe der Bestandsdaten nach § 14 Absatz 2 TMG. So besteht auch die Möglichkeit der Herausgabe der Verkehrsdaten und der Bestandsdaten in anonymen Mobile Payment Systemen. Aus diesem Grund soll dies bei der Gestaltung eines anonymen Mobile Payment Systems berücksichtigt werden

Die einzelnen Marktteilnehmer sollen bei den Klärungsprozessen der Rückverfolgung bzw. Strafverfolgung einbezogen werden. Insbesondere können hier der Anonymitätsservice, die TTP sowie der MNO große Hilfe leisten. Die Aufdeckung der Identität kann unter Umständen beispielsweise auch gegen Entgelt durch den Anonymitätsservice möglich sein. Bei der Gestaltung eines anonymen Mobile Payment Systems soll die Rolle und die Interessen der mobilen User berücksichtigt werden. Deshalb soll der mobile User bei einer Rückverfolgung bzw. Strafverfolgung wegen Betrugs- oder Missbrauchsfällen unterrichtet werden. Insbesondere kann eine Beteiligung des

---

622 Vgl. mit den Erläuterungen im Abschnitt 5.3.2.1 Vorratsdatenspeicherung und Überwachung der Netzwerke, S. 148.

623 Vgl. mit den Erläuterungen über das neue Urteil zur Vorratsdatenspeicherung vom 02.03.2010 im Abschnitt 5.3.2.1 Vorratsdatenspeicherung und Überwachung der Netzwerke, S. 148.

mobilen Users an der Klärung eines Missbrauchs oder eines Streits ermöglicht werden. Dabei soll der mobile User die Möglichkeit erhalten, eine Entschädigung für die Preisgabe der Identität zu erstreiten.

Zusammenfassend kann festgehalten werden, dass die regulatorischen Rahmenbedingungen zusammen mit den EU-Datenschutzrichtlinien bei der rechtlichen Gestaltung der anonymen Mobile Payment Systeme berücksichtigt werden sollen. Außerdem sollen neue Gesetze geschaffen oder der vorhandene Gesetzesrahmen modifiziert werden, da veränderte oder neu geschaffene mobile Anwendungen bzw. Payment Systeme dies erfordern. Mit dem letzten Urteil zur Vorratsdatenspeicherung ist es außerdem klar geworden, wie sich die Gesetze und Regeln entsprechend den Entwicklungen verfassungsmäßig gestaltet werden müssen.[624]

7.6 Mögliche Risiken und Probleme bei der Gestaltung

In den vorangegangenen Kapiteln und Abschnitten wurden bereits die Aspekte der Gestaltungsmöglichkeiten eines anonymen Mobile Payment Systems erläutert. Bei der Gestaltung eines anonymen Mobile Payment Systems und Prozesses können jedoch auch eine Reihe von Fragen, Probleme, Risiken und Gefahren auftreten. Nun sollen die kritischen Merkmale und Probleme sowie deren Lösungsmöglichkeiten im anonymen Mobile Payment System gezeigt werden, die in drei Hauptkategorien wie folgt eingestuft werden können:

- organisatorische Risiken und Probleme
- technische Risiken und Probleme
- regulatorische Risiken und Probleme

Die Identifizierung dieser Fragen und Probleme sowie Risiken und Gefahren werden im Folgenden detailliert dargestellt. Außerdem wird erklärt, welche Lösungsmöglichkeiten dafür existieren.

---

[624] Vgl. o. V. (2010d); Müller (2010a); Müller (2010b) sowie mit den Erläuterungen über das neue Urteil zur Vorratsdatenspeicherung vom 02.03.2010 im Abschnitt 5.3.2.1 Vorratsdatenspeicherung und Überwachung der Netzwerke, S. 148.

7.6.1 Organisatorische Risiken und Probleme

Bei der Gestaltung der User-Anonymität in Mobile Payment Systemen können organisatorische Probleme und Risiken auftauchen, mit denen sich die Anwender[625] des Referenzprozessmodells konfrontiert sehen können. Wenn die Anwender des Referenzprozessmodells ihre organisatorische Infrastruktur und Geschäftsprozesse ändern sollen, dann sollten sie entsprechende Strategien entwickeln, um zu planen, wie die anonymen Mobile Payment Prozesse angepasst werden bzw. wie die Einkaufs- und Payment-Prozesse organisiert werden können.

Wenn die einzelnen Prozesse geändert bzw. angepasst werden sollten, kann es sein, dass entsprechende organisatorische Infrastrukturen eingerichtet werden müssen, die eine finanzielle Investition erfordern. Die Frage ist, ob die Anwender des Referenzprozessmodells für eine solche Investition bereit sind, da der M-Commerce noch nicht seine Marktreife erreicht hat und deshalb die Gewinne in diesem Bereich trotz Vorhersage optimistischer Geschäftsentwicklungen nicht befriedigend sind. Außerdem gibt es Sicherheitsrisiken, die sich aus der Nutzung des Anonymitätsservice ergeben. Was würde passieren, wenn das Mobilfunkgerät verloren ginge, gestohlen und missbraucht würde? Problematisch kann es unterdessen sein, wenn die User falsche oder unbeabsichtigte Transaktionen tätigen. Es kann zum Vertrauensbruch bzw. zu Akzeptanzproblemen führen, wenn sich der Anonymitätsservice nicht als vertrauenswürdig genug erweist. Darüber hinaus basiert die Zahlungskultur in Deutschland auf Bargeld. Die Vorteile des Bargeldes liegen auf der Hand. Bei Zahlungstransaktionen mit Bargeld entstehen für den User keine oder niedrige Transaktionskosten. Der Datenschutz (Anonymität des Bargeldes) ist im vollen Umfang gewährleistet und Bargeld ist sofort verfügbar. Die Frage stellt sich, warum sollte der User ein Produkt oder einen Service mit seinem Mobilfunkgerät, möglicherweise mit zusätzlichen Transaktionskosten bezahlen, während dies mit dem Bargeld/Cash ohne Kosten geschieht? Warum sollte der User Mobile Payment präferieren, wenn dies Datenschutzrisiken darstellt, da der User mit der Nutzung vom Mobile Payment Spuren im Cyberspace hinterlässt. Was spricht für Mobile Payment, wenn die Bezahlung mit dem Bargeld sofort ohne irgendeine notwendige Bearbeitung erfolgen kann?

---

[625] Gemeint ist hier nicht der mobile User, der das anonyme Mobile Payment benutzt, sondern die Experten, die das Referenzprozessmodell in ihre IT-Systeme integrieren bzw. weiterentwickeln und dies zu den Endusern anbieten.

Risiken und Probleme können bei der Gestaltung des Trennungsprozesses der personenbezogenen Daten von den Payment-Transaktionsdaten auftreten. Die Prozessbeteiligten sollen nur die Daten des Users erhalten, die für die legitime Geschäftsabwicklung erforderlich sind. Diese Daten sind Transaktionsdaten, die im Einkauf- und Payment-Prozess anfallen. Die personenbezogenen Daten werden nur an Vertrauensinstanzen, also beim Mobilfunknetzbetreiber, Anonymitätsservice und der TTP gespeichert. Händler bzw. MCP und andere Marktteilnehmer sollen keine personenbezogenen Daten erhalten. Wenn die unnötigen Daten gespeichert werden, wird die Anonymität des Users beeinträchtigt. Dabei soll die Frage erörtert werden, ob diese Anforderung im Einklang mit der Verhältnismäßigkeit der Erhebung und Nutzung der Userdaten ist. Auf der anderen Seite soll der MCP in der Lage sein, seine Zahlungsforderungen gegenüber dem User jederzeit geltend machen kann. Bei der Gestaltung des Trennungsprozesses soll das Ausfallrisiko für den Händler mit berücksichtigt werden. In solchen Fällen soll der Anonymitätsservice eine Rückverfolgung der Identität des Users ermöglichen.[626]

Risiken und Probleme können bei der Gestaltung des Lieferungsprozesses physischer Produkte auftreten. Bei der Lieferung physischer Produkte kann die Identität des Users durch die Weitergabe des Namens und der Useranschrift bzw. Wohnadresse enthüllt werden. Bei der Lieferung digitaler Produkte tritt das Problem nicht auf, da die Lieferung nicht an die Wohnadresse sondern an die Mobilfunknummer erfolgt. Allerdings soll darauf geachtet werden, dass es keine Verkettung zwischen den Lieferungen digitaler und physischer Produkte und Services miteinander möglich ist. Wie bereits erläutert wurde, soll eine Kooperation zwischen dem Händler und Lieferunternehmen erschwert werden, so dass sie keine Daten und Informationen über den User tauschen können.[627]

Bei der Einrichtung eines Anonymitätsservices und einer Trusted Third Party wurde bereits betont, dass die Unabhängigkeit des Anonymitätsservices und der Trusted Third Party für das Vertrauen an anonyme Mobile Payment Systeme entscheidend sind. Aus diesem Grund stellt sich bei der Einrichtung des Anonymitätsservices sowie der TTP die Frage, wer oder welche Institutionen einen Anonymitätsservice errichten dürfen. Was würde passieren, wenn sich der Anonymitätsservice nicht als

---

[626] Vgl. mit den Erläuterungen im Abschnitt 7.3.1 Trennung der personenbezogenen Daten von den Transaktionsdaten, S. 179.

[627] Vgl. mit den Erläuterungen im Abschnitt 7.3.2 Berücksichtigung der Besonderheiten digitaler und physischer Produkten, S. 180.

vertrauenswürdig genug erweist? In einem solchen Fall kann es zum Vertrauensbruch bzw. Akzeptanzproblemen bei den anonymen Mobile Payment Systemen kommen. Deshalb müssen Anonymitätsservices für den User von den unabhängigen Institutionen angeboten werden.[628]

Bei der Realisierung des Referenzprozessmodells können Fragen, Probleme und Risiken wegen der erforderlichen Prozessänderungen seitens der einzelnen Marktteilnehmer auftauchen. Beispielsweise kann die fehlende Bereitschaft der einzelnen Marktteilnehmer, die notwendigen (Prozess-)Änderungen in einem anonymen Mobile Payment System vorzunehmen, die Gestaltung der User-Anonymität beeinträchtigen. Deshalb ist es erforderlich, die User-Anonymität in Mobile Payment Systemen als einen Mehrwert für den mobilen User von den einzelnen Marktteilnehmern zu fördern, um die Kundenzufriedenheit zu erhöhen. Im Einzelnen können bei der Realisierung des Referenzprozessmodells folgende Fragen, Probleme und Risiken auftauchen:[629]

Probleme und Risiken auf der Seite des mobilen Users: In diesem Zusammenhang ist die Bereitschaft der mobilen User enorm wichtig, an einem anonymen Mobile Payment System teilzunehmen und die erforderlichen Prozessanpassungen und deren Ausstattung dafür vorzunehmen. Außerdem ist das Problem der Akzeptanz eines neuen anonymen Mobile Payment Systems durch die User ernst zu nehmen. Das neue anonyme Mobile Payment System soll ein solides Vertrauen bei den Usern schaffen. Dieses solide Vertrauen am anonymen Mobile Payment System und seinen Prozessen kann durch die Sicherheit, Einfachheit und niedrigen Anschaffungs- und Transaktionskosten geschaffen werden. Wenn die anonymen Mobile Payment Prozesse so komplex gestaltet würden, könnte dies zur Ablehnung durch die User führen. Daher soll die Komplexität des neuen Mobile Payment Systems möglichst niedrig gehalten werden, so dass die Nutzung des MP Systems für die User anwenderfreundlich und attraktiv ist. Die Kostenfrage ist hier von besonderer Relevanz, als wenn die Prozesse bestehen und das System schon benutzt wird. Die Transaktionskosten entstehen sowohl in der Implementierungsphase als auch in der Nutzungsphase. Nicht außer Acht zu lassen ist die Frage, wer für die

---

[628] Vgl. mit den Erläuterungen über den Anonymitätsservice im Abschnitt 7.3.3 Einrichtung eines Anonymitätsservices, S. 182 und über die TTP im Abschnitt 3.1.7 Trusted Third Party, S. 60 sowie über die einzelnen Anonymitätskonzepte im Abschnitt 5.2.4 Anonymitätskonzepte, S. 124.

[629] Vgl. mit den Erläuterungen im Abschnitt 7.3.6 Erforderliche Prozessanpassungen seitens der Markteilnehmer, S. 185.

Transaktionskosten aufkommen soll. Soll der User hierfür verpflichtet werden oder der Anonymitätsservice selbst? Wenn ja, wie hoch fallen die Kosten aus? Hierfür sollen schon in der Konzept- bzw. Designphase eines anonymen Mobile Payment Systems Kostenkalkulationen für verschiedene Szenarien wie z. B. Mobile Payments in LBS etc. durchgeführt werden, um einzuschätzen, wie hoch die Kosten in Form der Nutzungsgebühren entstehen können, wenn es gebührenpflichtige Mobile Payment bzw. Anonymitätsservice angeboten werden sollen. Allerdings soll auch überlegt werden, ob dies nicht anders finanziert bzw. unentgeltlich für den User angeboten werden kann.[630]

Probleme und Risiken auf der Seite des Mobilfunknetzbetreibers können im Zusammenhang mit den übertragenen bzw. nicht übertragenen Daten sowie mit der Preisgabe der User-Identität auftauchen. Beispielsweise kann der MCP bezüglich der User-Identität den MNO konsultieren, wer z. B. hinter einem Pseudonym versteckt ist. Eine illegale Kooperation zwischen dem MCP und MNO kann in diesem Zusammenhang zu Vertrauensproblemen bei den Usern führen. Dies sollte verhindert bzw. verboten werden, solange beide Marktteilnehmer in ihren Mobile Payment Prozessen nicht beeinträchtigt werden. Auf der anderen Seite soll der User durch die Nutzung eines Anonymitätsservices den MNO nicht in Schwierigkeiten bringen.[631]

Das erste Risiko bzw. Problem bei den Prozessanpassungen des Anonymitätsservices ist die Sicherheit des Anonymitätsservices sowie die Schaffung des Vertrauens bei den Marktteilnehmern. Entscheidend ist auch die Legitimierung eines Anonymitätsservices. Die Zurückhaltung der personenbezogenen Daten soll garantiert werden. Eine Zusammenarbeit zwischen dem Anonymitätsservice und anderen Marktteilnehmern kann, zu Ungunsten der User, das Vertrauen und die Akzeptanz beeinträchtigen.[632]

Probleme und Risiken auf der Seite des MCP können in Form von Betrug, Missbrauch und Missverständnissen durch den User auftreten. Auf der anderen Seite kann der MCP die Nutzung eines Anonymitätsservices in seinen Mobile Payment

---

630 Vgl. mit den Erläuterungen im Abschnitt 3.2.3.2 Wirtschaftliche Anforderungen, S. 71 und im Abschnitt 3.2.4.1 Anforderungen der mobilen User, S. 72 sowie im Abschnitt 7.3.3 Einrichtung eines Anonymitätsservices, S. 182.

631 Vgl. mit den Erläuterungen im Abschnitt 3.2.4.3 Anforderungen anderer Marktteilnehmer, S. 77 und im Abschnitt 7.3.6.2 Prozessanpassungen des Mobilfunknetzbetreibers, S. 187.

632 Vgl. mit den Erläuterungen im Abschnitt 7.3.3 Einrichtung eines Anonymitätsservices, S. 182 und im Abschnitt 7.3.6.3 Prozessanpassungen des Anonymitätsservices, S. 187.

Prozessen verhindern, unterbinden oder verbieten. Er kann unbedingt verlangen, dass der User seine Identität preisgibt, also seine personenbezogenen Daten an den MCP zu übertragen. Der MCP soll sich überlegen, was geschäfts- sowie gesetzmäßig ist. Solange er seine Leistungen an den User bringen, abrechnen und das Geld eintreiben kann, ist die wahre Identität des Users zweitrangig. Außerdem kann er weiterhin Geschäftsanalysen machen, ohne die verkauften Produkte und Services den bestimmten Usern zuordnen zu können.[633]

Probleme und Risiken auf der Seite der TTP können mit der Authentifizierung der User und anderer Marktteilnehmer auftreten. Dies soll jedoch im nächsten Abschnitt Technische Risiken und Probleme erörtert werden.

Probleme und Risiken auf der Seite der Empfänger-Bank können im Überweisungs- und Begleichungsprozess nicht zu erwarten sein. Wenn Überweisungen vom Mobilfunknetzbetreiber (bzw. vom User) und Leistungen an den User abgeglichen werden, erfolgen die Zuordnung der Leistungen und dessen Zahlungen nach dem Pseudonym der User.[634] Probleme und Risiken können z. B. in Form der Fehlüberweisungen auftreten, weil z. B. das Pseudonym des Users nicht richtig angegeben bzw. falsch ist etc. In diesem Fall soll die Schadenersatzfrage beantwortet werden. Die Empfänger-Bank hat hier keine Abgleichpflicht bei Online-Überweisungen. Im Schadensfall kann die Verantwortung unter Umständen der Mobilfunknetzbetreiber übernehmen.[635]

7.6.2 Technische Risiken und Probleme

Bei der Gestaltung eines anonymen Mobile Payment Systems können einige technische Risiken und Probleme auftreten. Beispielweise können Probleme und Risiken bei der technischen Gestaltung des Anonymitätsservices in Form der Auswahl und der Implementierung der geeigneten Anonymitätstechniken auftauchen, da

---

633 Vgl. mit den Erläuterungen im Abschnitt 3.2.4.2 Anforderungen der Händler, S. 75 und im Abschnitt 7.3.6.4 Prozessanpassungen des Mobile Content Providers, S. 188.

634 Vgl. mit den Erläuterungen im Abschnitt 7.3.6.6 Prozessanpassungen der Bank, S. 189.

635 Im beleglosen Überweisungsverkehr, wie er beim Onlinebanking üblich ist, trifft die Empfängerbank keine Pflicht zum Abgleich zwischen Kontonummer und Empfängernamen. Dies hat das Amtsgericht München in einem jetzt veröffentlichten Urteil entschieden (Az.: 222 C 5471/07). Vgl. http://www.banktip.de/News/21954/Banken-muessen-Online-Ueberweisungen-nicht-abgleichen.html, Stand: 09.03.2010.

die Anonymitätstechniken in der Praxis bisher nicht oder wenig erprobt wurden.[636] Außerdem kann sich die technische Implementierung komplex darstellen. Die Komplexität einer Technik impliziert hohe Investitions- bzw. Wartungskosten, Fehlschlagungsgefahr, Performancemängel etc. Daher ist die Wahl der richtigen Anonymitätstechnik für die Errichtung und technische Gestaltung des Anonymitätsservices sehr kritisch. Falsche und mangelhafte Erfassung und Interpretation der Anforderungen zur Bestimmung der technischen Spezifikationen können zu falschen und mangelhaften technischen Spezifikationen führen. Dieses Risiko gilt auch für die Erfassung und Interpretation der organisatorischen und rechtlichen Anforderungen. Auf diese Weise können die Anforderungen der Marktteilnehmer nicht erfüllt werden und damit die Akzeptanz der User beeinträchtigt werden.

Fehlende IT-Infrastruktur oder ineffektive und ineffiziente IT-Infrastrukturen können ebenfalls zu technischen Problemen und Risiken in einem anonymen Mobile Payment System führen. Wenn die IT-Infrastrukturen für das Referenzprozessmodell fehlen, kann der Prozessablauf nicht organisiert werden. Auch wenn die Infrastrukturen vorhanden sind, kann es ein Problem sein, dass die Unterstützung der Prozesse durch die Marktteilnehmer fehlt. Die Frage stellt sich, was wird geschehen, wenn eine Verbindung während einer Transaktion abgebrochen wird? Oder was ist die Auswirkung, wenn die Übertragung von Authentifizierungsinformationen verzögert wird?

Ein erstes Problem kann bei der Authentifizierung des Users auftauchen. Wenn die Authentifizierung des Users wegen technischer Probleme wie Serverausfall oder der nicht kompatiblen Standards fehlschlägt, kann auch die Autorisierung des Services bzw. der Lieferung nicht erfolgen. Um dieses Risiko zu minimieren, sollen die Geschäftspartner ihre technischen Prozesse miteinander abstimmen, indem sie die Techniken und Standards von den Mobile Payment Initiativen anwenden bzw. sich mit ihnen kooperieren und ihre Erfahrungen austauschen sowie ihre Wünsche und eigene Vorschläge mitteilen.[637]

Bei der Gestaltung der Sicherheitsinstrumente wie die der Verschlüsselung der Kommunikation und Transaktionen sollen entsprechend den technischen Anforderungen richtige digitale Signierungs- und Verschlüsselungstechniken aus-

---

[636] Vgl. mit den Erläuterungen im Abschnitt 7.4.1 Technische Gestaltung eines Anonymitätsservices, S. 191 sowie im Abschnitt 7.4.2 Eignung und Übertragbarkeit der Anonymitätskonzepte, S. 191.

[637] Vgl. mit den Erläuterungen im Abschnitt 2.8 Mobile Payment Initiativen, S. 49

gewählt werden. Diese Auswahl kann in einer Selektion der Verschlüsselungstechniken oder in einer Kombination verschiedener Verschlüsselungstechniken durchgeführt werden. Auf diese Weise können die Anonymität der Kommunikations- und Transaktionsinhalte gewährleistet werden. Im Referenzprozessmodell wurde von dem Einsatz der asymmetrischen Verschlüsselungstechnik ausgegangen.[638]

Die Abstimmung der technischen Prozesse einzelner Marktteilnehmer entlang der Mobile Payment Wertschöpfungskette stellt einen kritischen Faktor dar. In jeder Phase der Mobile Payment Wertschöpfungskette sollen die einzelnen Prozesse gestaltet bzw. optimiert werden. Insbesondere in der technischen Gestaltung des Anonymitätsservices sollen Anonymisierung und Schlüsselübertragung miteinander abgestimmt werden. Wie bereits erläutert wurde, ist außerdem die Auswahl der richtigen Anonymitätstechnik sehr bedeutend. Daher soll die Eignung und Übertragbarkeit der Anonymitätstechniken genau analysiert werden. Die Verbindung der Trusted Third Parties ist ebenfalls entscheidend.[639]

Technische Risiken und Probleme können auch auf der Ebene der Applikationen entstehen. Die Installation, Konfiguration, Bedienung, Update sowie Lizenz einer Applikation stellen kritische Faktoren dar. Deshalb sollten sie den technischen Anforderungen der anonymen Mobile Payment Systeme entsprechen. Die technischen Prozesse, die mit der Applikation direkt zusammenhängen, sollen richtig gestaltet werden, damit eine reibungslose Vorbereitung, Bedienung und Problembehandlung möglich ist. Dies gilt auch für die Anforderungen technischer Ausstattung in anonymen Mobile Payment Systemen. Die Ermittlung und Bestimmung der technischen Spezifikationen bezüglich der Hardware und Software stellen sich als eine große Herausforderung für die Markteilnehmer dar, da ungeeignete Mobilfunkgeräte und Applikationen die Gestaltung der User-Anonymität in Mobile Payment Systemen gefährden können. Die Entwicklung geeigneter Mobilfunkgeräte und Applikationen kann in einer Kooperation der Marktteilnehmer besser durchgeführt

---

[638] Vgl. mit den Erläuterungen im Abschnitt 7.4.3 Berücksichtigung digitaler Verschlüsselungstechniken und Signaturen, S. 197.

[639] Vgl. mit den Erläuterungen im Abschnitt 7.4.2 Eignung und Übertragbarkeit der Anonymitätskonzepte, S. 191.

werden. Beispiel hierfür ist die Entwicklung der Java-Applikationen in den Java-fähigen Mobilfunkgeräten.[640]

Ein anderes entscheidendes Problem kann sich in der Geschwindigkeit der Transaktionsverarbeitung aufgrund der multiplen Prozessbeteiligten darstellen. Wenn mehrere Beteiligte an einem anonymen Mobile Payment Prozess teilnehmen, können sich ihre Prozesse entlang der Mobile Payment Wertschöpfungskette sehr komplex darstellen. Diese Komplexität kann unter den bereits gezeigten Rahmenbedingungen reduziert werden. Das heißt, die Marktteilnehmer können ihre Geschäftsprozesse intern und extern in organisatorischer und technischer Hinsicht optimieren und damit akzeptable Transaktionsgeschwindigkeiten erreichen.[641]

7.6.3 Regulatorische Risiken und Probleme

In den vorangegangenen Abschnitten wurden die regulatorischen Rahmenbedingungen sowie deren Berücksichtigung bei den Gestaltungsmöglichkeiten der User-Anonymität erörtert. Nun sollen die möglichen regulatorischen Risiken und Probleme bei der Gestaltung der User-Anonymität behandelt werden. Das erste Risiko könnte in der fehlenden Regulierung, also des fehlenden rechtlichen Rahmens und der Richtlinien, Gesetze und Verordnungen für die Gestaltung der User-Anonymität bestehen. Wenn der rechtliche Rahmen und die Bestimmungen fehlen, könnte es sein, dass die Aufsichtsinstanzen sowie Justiz- und Sicherheitsbehörden bei den anonymen Anwendungen und Transaktionen Mängel, Verdacht oder Verstoß feststellen und dadurch die Nutzung der Anonymitätsservices beschränken, wenn nicht gar verbieten.

Regulatorische Probleme und Risiken können in der Berücksichtigung gesetzlicher Rahmenbedingungen bei der Gestaltung der User-Anonymität auftreten. Beispielweise kann es bei der Entwicklung bzw. Errichtung des Anonymitätsservices zu Problemen mit der Anwendung und Einhaltung der behördlichen Richtlinien und rechtlichen Bestimmungen kommen. Wenn der Anonymitätsservice den Usern mit kriminellen Absichten Tür und Tor öffnet, kann er sofort gegen die gesetzlichen Bestimmungen verstoßen. Auf der anderen Seite kann es zu Problemen führen, wenn

---

[640] Vgl. mit den Erläuterungen im Abschnitt 7.1.2 Berücksichtigung und Erfüllung von technischen Anforderungen, S. 172 sowie im Abschnitt 7.1.3 Berücksichtigung und Erfüllung von funktionalen und wirtschaftlichen Anforderungen, S. 173.

[641] Vgl. mit den Erläuterungen im Abschnitt 7.6.1 Organisatorische Risiken und Probleme, S. 204.

die Vorbereitung und der Erlass von rechtlichen Bestimmungen und behördlichen Entscheidungen aufgrund des mangelndes Technik-Know-how nicht die Marktanforderungen erfüllen können oder den Marktbedürfnissen entsprechen. In einem solchen Fall sollen sich die Marktteilnehmer mit ihren Experten zusammenfinden, um entsprechende Lösungsmöglichkeiten zu erörtern. Beispielsweise können die Entwickler des Anonymitätsservices mit den Experten der Regulierungsbehörden schon in der Konzept- und Designphase eines anonymen Mobile Payment Systems zusammenarbeiten, um dessen Gesetzeskonformität zu erfüllen.[642]

Regulatorische Probleme und Risiken können auch bei strafrechtlichen Angelegenheiten in der Aufhebung und Aufdeckung der User-Anonymität auftreten. Beispielsweise kann der User sowie der Anonymitätsservice und andere Marktteilnehmer zu Schaden z. B. in Form der Verletzung der Persönlichkeitsrechte oder finanziellen Verlusten kommen, wenn die Aufdeckung der User-Anonymität nicht gesetzmäßig erfolgt oder nicht mit dem richterlichen Beschluss stattfindet. Wie bereits erläutert wurde, sollen die einzelnen Marktteilnehmer in solchen Fällen in die Klärungsprozesse der Rückverfolgung bzw. der Strafverfolgung einbezogen werden.[643]

Ein anderes Problem liegt in der Speicherung und Verwendung der Daten und damit in der Möglichkeit der Überwachung des Users in seinen Mobile Payment und bei anderen Aktivitäten wie Surfen, Informationsschaffung etc. Beispielsweise kann der User eine Verletzung seiner Persönlichkeitsrechte sehen, wenn die Speicherung und Verwendung der Daten nicht gesetzmäßig erfolgt. Beispielsweise können die Payment-Daten der User mit anderen Marktteilnehmern z. B. Händler mit den Lieferunternehmen nicht gesetzeskonform geteilt und verwendet werden. Das heißt, die Herausgabe der Verbindungsdaten und Bestandsdaten nicht nur in den genannten Fällen, sondern auch für die geschäftlichen Zwecke erfolgt, auch wenn das Gesetz ausdrücklich die Nutzung der Möglichkeit der Anonymisierung oder Pseudonymisierung betont.[644] An dieser Stelle soll nochmals erwähnt werden, dass die Vorratsdatenspeicherung durch das Urteil vom 02.03.2010 durch das Bundesverfassungsgericht nicht verfassungsmäßig und damit zusammenhängenden Para-

---

642 Vgl. mit den Erläuterungen im Abschnitt 7.5.1 Berücksichtigung gesetzlicher Rahmenbedingungen, S. 199.

643 Vgl. mit den Erläuterungen im Abschnitt 7.5.2 Berücksichtigung strafrechtlicher Aspekte, S. 201 sowie Müller (2010b).

644 Vgl. mit den Erläuterungen im Abschnitt 7.5.2 Berücksichtigung strafrechtlicher Aspekte, S. 201.

graphen in den relevanten Gesetzen und Verordnungen nichtig sind.[645] Dieses Urteil hat die Konsequenzen für die Marktteilnehmer, insb. für den Gesetzgeber und die Service Provider.[646] Der Gesetzgeber muss diese Gesetze verfassungskonform gestalten. Die Service Provider müssen die gespeicherten Daten unverzüglich löschen. Dies zeigt auch das Risiko, dass die regulatorischen Änderungen oder die unklaren Regeln hohe Planungs- und Investitionskosten verursachen, da die Service Provider hohe Investitionen in ihre IT-Systeme für die Speicherung der Daten getätigt hatten.[647]

[645] Vgl. mit den Erläuterungen zum Bundesverfassungsurteil vom 02.03.2010 im Abschnitt 5.3.2 Strafrechtliche Aspekte der User-Anonymität, S. 148 sowie im Abschnitt 7.5.2 Berücksichtigung strafrechtlicher Aspekte, S. 201

[646] Vgl. Müller (2010b).

[647] Vgl. o. V. (2010d).

8 Fazit

In diesem Kapitel wird zunächst eine kurze und präzise Zusammenfassung der zentralen Aussagen und der wichtigsten Ergebnisse dieser Dissertation dargestellt. Danach werden die Schlussfolgerungen aus den Ergebnissen der Arbeit abgeleitet. Schließlich wird ein Ausblick auf die offenen Fragen und weiteren Forschungsrichtungen gegeben, um zu zeigen, welche Themen im Bereich User-Anonymität und Mobile Payment Systeme für die weiteren Forschungen interessant sein können.

8.1 Zusammenfassung

Der Schutz der persönlichen Daten vor Manipulation und Missbrauch gewinnt in mobilen Kommunikationsnetzwerken immer mehr an Bedeutung. Immer mehr Menschen machen sich Gedanken bezüglich der persönlichen Daten und Informationen, die sie im Mobile Commerce und Mobile Payment hinterlassen. Sie fragen sich oft, was mit hinterlassenen Daten und Informationen geschieht, wenn sie Mobile Payments nutzen. Es fehlt die User-Anonymität in den vorhandenen Mobile Payment Systemen. Aus diesem Grund stellt die User Anonymität eine wichtige Anforderung dar und bietet einen enormen Kundennutzen für die Akzeptanz und Nutzung von Mobile Payment. Deshalb wurden in dieser Dissertation auf diese Anforderung des Users und ihre Fragestellungen näher eingegangen. Die Ergebnisse können wie folgt zusammengefasst werden:

Zuerst wurde ein Überblick über die Mobile Payments, die Marktteilnehmer und deren Interessen und Anforderungen gegeben. Die rasanten Entwicklungen im Bereich „Mobile“ bzw. M-Commerce erfordern demnach effektive und effiziente Mobile Payment Systeme. Diese können für alle Typen von Einkäufen eingesetzt werden, speziell im Bereich der Micro Payments, aber auch im Bereich der Macro Payments. Mobile Payment Systeme basieren auf der Infrastruktur der Banken bzw. Kreditkartengesellschaften, Mobilfunknetzbetreiber sowie innovativen Internet-Unternehmen wie Google, eBay und Amazon etc. Es dürfte sehr wahrscheinlich sein, dass diese breite Basis verschiedener Systeme parallel existieren wird, da sich die Banken, Kreditkartengesellschaften, Mobilfunknetzbetreiber und innovativen Internet-Unter-nehmen für Mobile Payments interessieren, wenn auch mit unterschiedlicher Hingabe. Speziell jedoch haben die Kreditkartengesellschaften und Mobilfunknetzbetreiber große Chancen, aus Gründen der Internationalität, Kompetenz und

strategischer Bedeutung, eine dominierende Rolle in den Mobile Payment Systemen zu spielen. Das Mobile Payment Ökosystem besteht aus verschiedenen Marktteilnehmern und Interessensgruppen, die verschiedene Anforderungen an die Mobile Payment Systeme stellen. Bei der Gestaltung der Mobile Payment Systeme sollen diese Anforderungen nach den Interessen der Marktteilnehmer im Mobile Payment Ökosystem in einer gesunden Balance berücksichtigt werden. Spezielles Hauptaugenmerk soll jedoch auf die Anforderungen mobiler User gerichtet werden, da die Mobile Payment Systeme erst durch die Befriedigung der User-Erwartungen und die Erfüllung der User-Anforderungen eine breite Akzeptanz finden. Die User-Anonymität ist eine dieser Anforderungen. Erst wenn unter anderem diese Anforderung des Users erfüllt werden kann, können Mobile Payment Systeme eine breite Akzeptanz bei mobilen Usern finden.

Für ein besseres Verständnis wurde auf das Thema der Anonymität eingegangen. Anschließend wurde die Bedeutung der User-Anonymität in Mobile Payment Systemen gewürdigt. Die Anonymität stellt sich als ein wichtiges Schutzziel der Vertraulichkeit der Informations- und Kommunikationssysteme dar.

Anonymität bedeutet, dass der Absender bzw. Empfänger einer Nachricht innerhalb einer Menge möglicher Absender bzw. Empfänger nicht identifizierbar sind. Die User können bestimmte Anwendungen benutzen und Dienstleistungen von Dritten in Anspruch nehmen, ohne dass sie ihre Identität offenbaren müssen.

Bei der Informationssicherheit geht es um den Schutz vor Gefahren und Bedrohungen sowie die Vermeidung von Schäden und die Minimierung von Risiken für Informationssysteme. Beim Datenschutz geht es hauptsächlich um den Schutz personenbezogener Daten vor Manipulation bzw. Missbrauch. Personenbezogene Daten beschreiben persönliche oder sachliche Verhältnisse einer natürlichen Person.

Für und wider die Anonymität werden verschiedene Argumente erhoben. Der Schutz der Privatsphäre der Personen in den stationären und mobilen Kommunikationsnetzen soll genau so wie im realen Leben gewährleistet und sowohl organisatorisch und technisch als auch rechtlich adäquat gestaltet werden. Auf der anderen Seite kann die Anonymität unter Umständen Schutz für kriminelle Personen bieten und von kriminellen Personen oder Gruppen missbraucht werden, um Verbrechen zu begehen.

Es gibt verschiedene Formen der Anonymität in den Kommunikationsnetzwerken. Die Form der Anonymität wird durch die verschiedene Faktoren und Umstände in

den Kommunikationsnetzwerken bestimmt. Es wurde gezeigt, welche Formen der Anonymität existieren, welchen Umfang sie einnehmen und welche Unterschiede zwischen den Formen der Anonymität bestehen. Danach kann zunächst zwischen der Prozessanonymität, Kommunikationsanonymität und Ortanonymität unterschieden werden. Diese können wiederum in Senderanonymität, Empfängeranonymität, Client-, Server- und Contentanonymität unterteilt werden.

Der User besitzt verschiedene Identitäten entsprechend seinen Rollen und Taten in der Gesellschaft. Diese Identitäten lassen sich in vier Gruppen, nämlich in persönliche, physische, digitale und virtuelle sowie multiple Identitäten, klassifizieren. Darüber gibt es in einer Transaktion grundsätzlich drei Anonymitätsgrade, die anhand der Bekanntheit der Beteiligten in absolute Identität (keine Anonymität), Teilidentität oder Pseudonymität (partielle Anonymität) sowie absolute Anonymität unterteilt werden können. Es gibt im Verfahren der Pseudonymisierung drei Pseudonyme, die eine partielle Anonymität und gleichzeitig, je nach dem, eine Rückidentifizierung einer Person erlauben. Diese sind usererstellte, Referenz- und Einweg-Pseudonyme.

Aus soziologischer Sicht ermöglicht die Anonymität auf individueller Ebene eine gewisse Unabhängigkeit und Freiheit, auf sozialer Ebene eine Wahlmöglichkeit zwischen den Alternativen. Aus ökonomischer Sicht braucht man nicht immer auch persönliche Daten zu tauschen. Eine wichtige Eigenschaft des Bargeldes ist seine Anonymität. Zwischen den Zahlungen und den gekauften Produkten kann keine Beziehung hergestellt werden. Der mobile User würde gerne diese Eigenschaft des Bargeldes auch in Mobile Payment Systemen wiederfinden. So können das Vertrauen der Kunden in Mobile Payments und damit die Akzeptanz der Mobile Payments erhöht werden.

In dieser Dissertation sollten neue Paradigmen, die zur Lösung der Problematik beitragen, entwickelt bzw. angewendet werden. Hierfür wurden die Rahmenbedingungen zur Herstellung und Bewahrung der User-Anonymität gezeigt. Ferner wurden die Gestaltungsmöglichkeiten zur Vermeidung der Beobachtung des Userverhaltens und Verkettung der Daten und Informationen untersucht. Diese ergeben sich aus organisatorischen, technischen und regulatorischen Rahmenbedingungen. Hierfür wurden die vorhandenen und neuen potentiellen Gestaltungsmöglichkeiten zur User-Anonymität untersucht.

Die organisatorischen Gestaltungsmöglichkeiten drücken sich in der Organisation und Behandlung verschiedener Daten und Informationen sowie in der Organisation

und Gestaltung der Prozesse aus. Hierfür wurden die Organisation und Behandlung der Bestanddaten und personenbezogenen Daten sowie der Verbindungsdaten und Transaktionsdaten untersucht. Die Behandlung der Daten und Informationen ist gesetzlich geregelt. Dies wurde in den regulatorischen Rahmenbedingungen näher erläutert.

Die technischen Gestaltungsmöglichkeiten sind vielfältig und lassen sich auf verschiedenen Gestaltungsebenen anwenden. Neben den anonymen Protokollen und Server Systemen gibt es auch Anonymitätskonzepte. Speziell bieten die Anonymitätskonzepte der Mixe oder mCrowds verschiedene Gestaltungsmöglichkeiten zur User-Anonymität bzw. Errichtung eines Anonymitätsservices.

Die regulatorischen Rahmenbedingungen bestehen aus den EU- und bundesdeutschen Datenschutzrichtlinien sowie den Gesetzen und Verordnungen. Diese Richtlinien, Gesetze und Verordnungen stellen regulatorische Rahmenbedingungen für die Marktteilnehmer in der Telekommunikation bereit. Die regulatorischen Rahmenbedingungen bestimmen die Gestaltungsmöglichkeiten rechtlich konformer User-Anonymität in Mobile Payment Systemen.

Auf der Grundlage der Rahmenbedingungen wurden die verschiedenen Lösungsansätze, die zur Gestaltung der User-Anonymität beitragen, miteinander verknüpft, um ein ideales und optimales Modell zur anonymen Mobile Payment aufzustellen. Hierfür wurden die auf dem Markt befindlichen Mobile Payment Systeme und deren Prozesse und Anonymität untersucht. Auf der Basis eines Praxisbeispiels, Mobile Content Download, wurde ein Referenzprozessmodell zur User-Anonymität entwickelt.

Das in dieser Dissertation vorgeschlagene Referenzprozessmodell ermöglicht es den mobilen Usern, dass sie anonyme Mobile Payments tätigen können, ohne dabei ihre Identität bei den Händlern preiszugeben. Das Referenzprozessmodell wurde mit Hilfe der Heranziehung der existierenden Anonymitätskonzepte entwickelt, die die Möglichkeit zur Gestaltung anonymer Kommunikation und Transaktionen in den (mobilen) Netzwerken bieten. Das Referenzprozessmodell wurde so entwickelt, dass die User-Anonymität einfach und mit einem minimalen Aufwand hergestellt werden kann. Der mobile User ist damit in der Lage, selber zu entscheiden, ob, wann und in welchen Situationen er anonym bleiben möchte.

Für die Realisierung des Referenzprozessmodells wurden Wege nach effektiven und effizienten Werkzeugen und Technologien gezeigt. Hierfür wurde dargestellt, welche

organisatorischen, technischen und regulatorischen Maßnahmen getroffen werden sollen, um das Referenzprozessmodell zu realisieren und damit einen bestimmten Grad an der User-Anonymität bei Mobile Payment Systemen herzustellen. Neben den verschiedenen Gestaltungsmöglichkeiten wurden die potentiellen Risiken und Probleme, die bei der Realisierung auftauchen können, dargestellt.

Für die Realisierung des Referenzprozessmodells wurden die Berücksichtigung und Erfüllung der Anforderungen und Rahmenbedingungen detailliert aufgezeigt. Hierfür wurden die organisatorischen, technischen und regulatorischen Gestaltungsmöglichkeiten bewertet sowie Wege für die Realisierung des Referenzprozessmodells gezeigt, wobei der Fokus auf die organisatorischen Maßnahmen gesetzt wurde. Für die organisatorische Realisierung des Referenzprozessmodells wurden die folgenden Gestaltungswege dargelegt:

Trennung der Daten bzw. getrennte Behandlung von Daten: Die User-Anonymität in Mobile Payment Systemen kann nur dadurch hergestellt werden, wenn die personenbezogenen Daten von den Transaktionsdaten getrennt und so behandelt werden. Dies ist auch gesetzlich vorgeschrieben. Im Referenzprozessmodell erhält der MCP bzw. Händler keine personenbezogenen Daten des Users, sondern anonymisierte Userdaten und Informationen.

Besonderheiten digitaler und physischer Produkte: Bei der Lieferung der digitalen und physischen Produkte an den mobilen User bzw. die Adresse des mobilen Users gibt es eine Besonderheit, die bei der Gestaltung der User-Anonymität berücksichtigt werden sollte. Die Lieferung der digitalen Produkte erfolgt an das Mobilfunkgerät des Users, während das physische Produkt an die Adresse des Users geliefert oder am POS im Geschäft persönlich ausgehändigt wird. In den genannten Fällen können sowohl der MCP als auch der Händler die gelieferten Produkte den Usern zuordnen. Im Referenzprozessmodell hat der mobile User die Möglichkeit, seine Identität durch einen Anonymitätsservice zu managen. Auf diese Weise werden keine personenbezogenen Daten des Users an den MCP bzw. Händler übertragen. Sie erhalten nur anonymisierte Userdaten und -Informationen.

Einrichtung eines Anonymitätsservices und einer TTP: Für die organisatorische Gestaltung eines anonymen Mobile Payment Systems ist die Einrichtung eines Anonymitätsservices sowie einer TTP entscheidend, da der mobile User erst durch die Nutzung dieses Anonymitätsservices anonyme Mobile Payment durchführen kann.

Die Einrichtung eines Anonymitätsservices kann beispielsweise sowohl als ein neues Geschäftsmodell als auch durch die Mobilfunknetzbetreiber als Vermittlungs- bzw. Vertrauensstelle für anonyme Zahlungstransaktionen zwischen den mobilen Usern und MCP geschehen. Dadurch kann auch der Prozess der Zahlungstransaktionen vereinfacht werden, etwa durch die Nutzung der eigenen internen Billing-Infrastruktur. Das heißt, der Mobilfunknetzbetreiber kann z. B. als eine Payment Mediation auftreten.

Neben der Einsetzung eines Anonymitätsservices soll für die Gestaltung eines anonymen Mobile Payment Prozesses eine TTP eingesetzt werden, die für die Zertifizierung und Durchführung der Authentifizierung der Transaktionsparteien zuständig ist. In einem Mobile Payment System können die Mobilfunknetzbetreiber, Banken oder Kreditkartengesellschaften die Rolle einer TTP übernehmen, da sie ohnehin das Vertrauen von Transaktionsparteien genießen.

Die Vertrauensfrage und Unabhängigkeit des Anonymitätsservices sowie der TTP ist für die Gestaltung eines anonymen Mobile Payment Systems sehr wichtig. Deshalb soll die Unabhängigkeit der beiden Parteien bei der Gestaltung des anonymen Mobile Payment Prozesse gegeben sein oder möglichst durch die regulatorischen Maßnahmen gesichert werden. Beide Dienste sollen die Nutzung der Services und die Steigerung des Vertrauens in ihre Services durch eine sichere, bequeme und flexible Umgebung ermöglichen.

Prozessanpassungen der Marktteilnehmer: Für die Gestaltung der User-Anonymität im anonymen Mobile Payment System sind einige Prozessanpassungen seitens der einzelnen Marktteilnehmer, nämlich seitens des Users, des Mobilfunknetzbetreibers, des Anonymitätsservices, des Mobile Content Händlers, der Bank und TTP sowie der übrigen Prozessbeteiligten, in unterschiedlichen Maßen erforderlich.

Neben den organisatorischen wurden die technischen Gestaltungsmöglichkeiten bewertet. Hierfür wurde zunächst die technische Gestaltung eines Anonymitätsservices gezeigt. Für die Gestaltung eines Anonymitätsservices sollen die vorhandenen Anonymitätstechniken und deren Anwendungen in der Praxis berücksichtigt werden. Hierfür wurden die Übertragbarkeit und Eignung der Anonymitätskonzepte bewertet. Anschließend wurden die Berücksichtigung digitaler Verschlüsselungstechniken und Signaturen für die personenbezogenen Daten und Transaktionsdaten betont. Außerdem wurde die Funktion der TTP bzw. Certification Authorities erwähnt.

Die Berücksichtigung der regulatorischen Rahmenbedingungen ist ein notwendiger Schritt für die Gestaltung der User-Anonymität in Mobile Payment Systemen. Hierfür wurden die gesetzlichen Grundlagen und strafrechtlichen Aspekte der User-Anonymität gezeigt. Die Prozessbeteiligten sollen in anonymen Mobile Payment Systemen nach den Datenschutzbestimmungen handeln. Insbesondere die gesetzlichen Datenschutzbestimmungen wie das Verbotprinzip mit Erlaubnisvorbehalt, Datenvermeidung und Datensparsamkeit spielen eine wichtige Rolle. Bei der Gestaltung eines anonymen Mobile Payment Prozesses sollen die strafrechtlichen Aspekte berücksichtigt werden. Bei der Gestaltung eines anonymen Mobile Payment Systems soll berücksichtigt werden, dass eine Aufdeckung bzw. Aufhebung der User-Anonymität bei Betrugs-, Missbrauchs- und Manipulationsfällen möglich ist. Der Gesetzgeber zwang bisher Service Provider, alle Kommunikationsvorgänge zu protokollieren und mindestens sechs Monate zu speichern. Die bisherigen Vorschriften zur Speicherung und Verwendung der Daten wurden durch das Bundesverfassungsurteil vom 02.03.2010 nicht als verfassungsmäßig entschieden. Danach dürfen Daten nur bei konkreten Verdachtsfällen zur Strafverfolgung und Gefahrenabwehr gespeichert werden. So wird es möglich sein, dass Daten, die in anonymen Mobile Payment Transaktionen auftauchen, nur für die genannten Fälle und Zwecke gespeichert werden dürfen. Für die Verfolgung und Aufklärung der Straftaten sowie für die Gefahrenabwehr mittels Telekommunikation besteht ein Anspruch, die Herausgabe der Verkehrsdaten zu fordern. So besteht auch eine Möglichkeit der Herausgabe der Verkehrsdaten und der Bestandsdaten in anonymen Mobile Payment Systemen. Die einzelnen Marktteilnehmer sollen bei den Klärungsprozessen der Rückverfolgung bzw. Strafverfolgung einbezogen werden. Insbesondere können hier der Anonymitätsservice, die TTP sowie der MNO große Hilfe leisten. Die Aufdeckung der Identität kann unter Umständen auch gegen Entgelt durch den Anonymitätsservice möglich sein. Bei der Gestaltung eines anonymen Mobile Payment Systems sollen die Rolle und die Interessen der mobilen User berücksichtigt werden.

Bei der Gestaltung eines anonymen Mobile Payment Systems und Prozesses können eine Reihe von Fragen, Probleme, Risiken und Gefahren auftreten. Hierfür wurden die kritischen Merkmale und Probleme sowie deren Lösungsmöglichkeiten im anonymen Mobile Payment System gezeigt. Diese wurden in drei Hauptkategorien, nämlich in organisatorische, technische und regulatorische Risiken und Probleme eingestuft und erläutert.

Organisatorische Probleme und Risiken können in der Planung und Implementierung der anonymen Mobile Payment Systeme auftreten. Wenn die einzelnen Prozesse geändert bzw. angepasst werden sollten, kann es sein, dass entsprechende organisatorische Infrastrukturen eingerichtet werden müssen, die eine finanzielle Investition erfordern. Risiken und Probleme können bei der Gestaltung des Trennungsprozesses der personenbezogenen Daten von den Payment-Transaktionsdaten sowie bei der Gestaltung des Lieferungsprozesses physischer Produkte auftreten. Wenn sich der Anonymitätsservice nicht als vertrauenswürdig genug erweist, kann es zum Vertrauensbruch bzw. Akzeptanzproblemen bei den anonymen Mobile Payment Systemen kommen. Bei der Realisierung des Referenzprozessmodells können Fragen, Probleme und Risiken wegen der erforderlichen Prozessänderungen seitens der einzelnen Marktteilnehmer auftauchen. Bei der organisatorischen Gestaltung der anonymen Mobile Payment Systeme sollen die Aspekte des Vertrauens, der Geschäftsabwicklung sowie -risiken wie z. B. die Gestaltung des Lieferungsprozesses, Ausfallsrisiko oder Schadenfallsregelung und Rückverfolgbarkeit der Identität des Users etc. berücksichtigt werden.

Technische Probleme und Risiken können in der Auswahl und Implementierung der geeigneten Anonymitätstechniken für die technische Gestaltung des Anonymitätsservices auftauchen, da die Anonymitätstechniken in der Praxis bisher nicht oder wenig erprobt wurden. Außerdem können falsche und mangelhafte Erfassung und Interpretation der Anforderungen zu falschen und mangelhaften technischen Spezifikationen führen. Dieses Risiko gilt auch für die Erfassung und Interpretation der organisatorischen und rechtlichen Anforderungen. Auf diese Weise können die Anforderungen der Marktteilnehmer nicht erfüllt werden und damit die Akzeptanz der User beeinträchtigt werden.

Regulatorische Probleme und Risiken können in der Berücksichtigung gesetzlicher Rahmenbedingungen sowie in den strafrechtlichen Angelegenheiten auftreten. Beispielweise kann es bei der Entwicklung bzw. Errichtung des Anonymitätsservices zu Problemen mit der Anwendung und Einhaltung der behördlichen Richtlinien und rechtlichen Bestimmungen kommen. Die rechtlichen Bestimmungen und behördlichen Entscheidungen können aufgrund des mangelndes Technik-Know-hows nicht die Marktanforderungen erfüllen oder den Marktbedürfnissen entsprechen. Außerdem können die regulatorischen Änderungen oder die unklaren Regeln hohe Planungs- und Investitionskosten verursachen. Ein anderes Problem liegt in der Speicherung und Verwendung der Daten und damit in der Möglichkeit der Über-

wachung des Users in seinen Mobile Payment und bei anderen Aktivitäten wie Surfen, Informationsschaffung etc.

8.2 Schlussfolgerung

Die vorliegende Dissertation sollte einen innovativen Beitrag zur Lösung der Problematik der User-Anonymität in Mobile Payment Systemen leisten. Es wurden potentielle Risiken und Gefahren erläutert sowie Anforderungen, Rahmenbedingungen und Gestaltungsmöglichkeiten der User-Anonymität anhand eines Praxisbeispiels in einem Referenzprozessmodell erklärt.

Der Schutz der persönlichen Daten vor Manipulation und Missbrauch gewinnt in mobilen Kommunikationsnetzwerken immer mehr an Bedeutung. Die User-Anonymität stellt daher eine ganz wichtige Anforderung für die Akzeptanz und Nutzung von Mobile Payments und bietet einen enormen Kundennutzen. Bei der Gestaltung der Mobile Payment Systeme sollen die Anforderungen aller Marktteilnehmer im Mobile Payment Ökosystem in einer gesunden Balance berücksichtigt und erfüllt werden. Die User-Anonymität ist eine dieser Anforderungen. Erst wenn die Anforderung des Users erfüllt werden kann, können die Mobile Payment Systeme eine breite Akzeptanz finden.

Die Anonymität stellt sich als ein wichtiges Schutzziel der Vertraulichkeit der Informations- und Kommunikationssysteme dar. Der Schutz der Privatsphäre der Personen in den stationären und mobilen Kommunikationsnetzwerken soll genau so wie im realen Leben gewährleistet und sowohl organisatorisch und technisch als auch rechtlich adäquat gestaltet werden. Zwischen den Argumenten für und gegen die Anonymität soll einen Kompromiss gefunden werden. Die Anonymität soll als ein gestalterisches Element vom System und der Sicherheit betrachtet werden. Die Anonymität soll daher in die (System-)Sicherheitspolitik und -richtlinien integriert werden.

Die verschiedenen Formen der Anonymität können durch die verschiedenen Grade der Anonymität beliebig hergestellt bzw. gestaltet werden. Diese Gestaltungsmöglichkeiten der Anonymität können auch für die User-Anonymität in Mobile Payment Systemen genutzt werden. Das Thema der User-Anonymität soll für M-Commerce, M-Payment und die mobilen Anwendungen als wichtiges Element betrachtet werden. Die mobilen Anwendungen sollen unter diesen Bedingungen gestaltet werden. Jeder soll dann in seiner informationellen Selbstbestimmung eine adäquate Option für die

gewünschte Identität bzw. Anonymität finden können. Wünschenswert ist eine (absolute) Anonymität, wie dies in der Anonymität des Bargeldes vorhanden ist. Das heißt, mobile User sollten Mobile Payments genauso wie in Bargeldzahlungen anonym durchführen können, wenn sie dies möchten. Die Einbeziehung der User-Anonymität sollte ein wichtiger und integraler Bestandteil bei der Entwicklung der anonymen Mobile Payment Systemen sein. Die Überlegungen bezüglich der User-Anonymität sollten schon in der Design-Phase der Entwicklungen der Mobile Payment Systeme einfließen.

Das in dieser Dissertation vorgeschlagene Referenzprozessmodell ermöglicht es den mobilen Usern, dass sie anonyme Mobile Payments tätigen können, ohne dabei ihre Identität bei den Händlern preiszugeben. Das Referenzprozessmodell dient der Entwicklung der anonymen Mobile Payment Prozesse und stellt ein spezielles Modell für den Entwurf und die Entwicklung weiterer Ideen und Modelle dar, die sich für die Gestaltung der User-Anonymität in Mobile Payment Systemen befassen. Eine Rückverfolgbare und widerrufliche User-Anonymität soll möglich sein, gefördert und weiterentwickelt werden. Für die Gestaltung eines Anonymitätsservices sollen die vorhandenen Anonymitätstechniken und deren Anwendungen in der Praxis berücksichtigt werden. Durch die technischen Möglichkeiten (Anonymitätskonzepte) kann User-Anonymität in Mobile Payment Systemen realisiert werden, um die Akzeptanz und das Vertrauen zu steigern.

Anonyme Mobile Payment Systeme müssen nach den aktuellen Datenschutzbestimmungen gestaltet werden. Dabei muss darauf geachtet werden, dass die einzelnen Prozessbeteiligten nur diejenigen Daten erhalten, welche sie für die Geschäfts- und Zahlungsabwicklung absolut benötigen. Sonst bestände die Gefahr, über die Zahlungstransaktionsdaten Userprofile mit Bewegungs- und Konsumverhalten zu erstellen. Die Prozessbeteiligten sollen in anonymen Mobile Payment Systemen nach den Datenschutzbestimmungen handeln. Insbesondere die gesetzlichen Datenschutzbestimmungen wie das Verbotprinzip mit Erlaubnisvorbehalt, Datenvermeidung und Datensparsamkeit spielen eine wichtige Rolle.

Mobile Payment Systeme müssen Usern einen bestimmten Schutz vor Missbrauch und Manipulation wie z. B. bei Verlust oder Diebstahl des Mobilfunkgerätes garantieren. Ein Mobile Payment System sollte grundsätzlich so ausgestaltet sein, dass die Gefahr eines finanziellen Verlustes des Users durch Manipulation oder Missbrauch möglichst gering ist. Der Datentransfer zwischen den einzelnen Marktteilnehmern sowie die verwendeten Technologien sollten die aktuellen Sicherheitsan-

forderungen erfüllen. Bei der Gestaltung eines anonymen Mobile Payment Systems soll berücksichtigt werden, dass eine Aufdeckung bzw. Aufhebung der User-Anonymität bei Betrugs-, Missbrauchs- und Manipulationsfällen möglich ist. Der regulatorische Rahmen soll im Sinne vom Schutz der User-Anonymität weiter entwickelt werden. Die vorhandenen Gesetze zum Datenschutz und zur Privatsphäre sowohl in Deutschland als auch auf europäischer Ebene weiterentwickelt werden. Gegebenenfalls sollen neue Gesetze, Verordnungen und Richtlinien erlassen werden.

Der mobile User muss aufgrund der Transparenz der anonymen Mobile Payment Systeme generell im Vorfeld darüber informiert werden, welche Daten zu welchem Zweck wann, wo und wie bearbeitet werden und welche Risiken bei der Nutzung der anonymen Mobile Payments entstehen können. Außerdem muss der mobile User über die Funktionsweise der anonymen Mobile Payment Systeme sowie über den Datentransfer in anonymen Mobile Payment Systemen in verständlicher Form informiert werden.

Die Themen User-Anonymität, Privatsphäre und Datenschutz spielen im gesellschaftlichen und privaten Leben eine große Rolle und sollen deshalb weiter diskutiert und weiter entwickelt werden. Ein Bewusstsein für das Thema der User-Anonymität soll speziell in Mobile Payment Systemen allgemein in der Gesellschaft gebildet werden. Jeder User sollte selber abwägen, in wie weit er personenbezogene Daten und Informationen an Dritte preisgibt. Eine absolute Anonymität ist nicht möglich oder mit großem Aufwand herzustellen.

8.3 Ausblick

In dieser Dissertation wurde ein organisatorisches Konzept zur Gestaltung der User-Anonymität in Mobile Payment Systemen herausgearbeitet, wobei dies eine Lösung auf einer hohen Abstraktionsebene (High-Level-Lösung) zur gestellten Problematik darstellt. Die organisatorischen Prozessanpassungen und Maßnahmen, die für die Gestaltung und Funktion der User-Anonymität in Mobile Payment Systemen erforderlich sind, wurden detailliert dargestellt. Das Referenzprozessmodell wurde in der Praxis noch nicht erprobt. Es handelt sich um ein Szenario zur User-Anonymität in Mobile Payment Systemen, in dem ein organisatorisches Konzept auf den Grundlagen der Anforderungen und der Rahmenbedingungen der User-Anonymität erarbeitet wurde. Die Bestimmung der technischen Spezifikationen hängt vom jeweiligen Mobile Payment System ab. In diesem Konzept wurde jedoch nicht auf

alle technischen und regulatorischen Fragen im Detail eingegangen. Zum einen ist die Beantwortung der technischen und regulatorischen Fragen im Detail nicht das Ziel der Untersuchung. Für die Beantwortung solcher Fragen wird auf die einschlägige Literatur verwiesen. Zum anderen hätte ein Versuch zur Beantwortung dieser Fragen den Rahmen dieser Dissertation gesprengt. Daher stellen die technischen und regulatorischen Fragen, die bisher nicht genannt worden bzw. offen geblieben sind, neue Herausforderungen zur weiteren Forschung in diesem Themengebiet dar. Nach der Untersuchung der Gestaltung und Machbarkeit der User-Anonymität wäre eine Richtung für eine weitere Forschung die Komplexitätsreduktion der Geschäftsprozesse, die eine User-Anonymität gewährleisten.

Literatur

Abrazhevich (2004): Abrazhevich, Dennis: Electronic payment systems: a user-centered perspective and interaction design, Eindhoven, Technische Universiteit Eindhoven, 2004.

Abts/Mülder (2009): Abts, Dietmar; Mülder, Wilhelm: Grundkurs Wirtschafts-informatik: Eine kompakte und praxisorientierte Einführung, 6. Auflage, Vieweg+Teubner-Verlag, Wiesbaden, 2009.

ACTiSYS (2002): IrFM (Inra-red Financial Messaging) Wireless Mobile Payment - Background and Market Status (as of Dec 2002), ACTiSYS Corporation, Fremont, CA, USA, 2002.

http://www.actisys.com/Documents/IrFmBackgroundMarket_030213.pdf, Stand: 19. 02.2010.

Adamec et al. (2009): Adamec, Pavol [u. a.]: Mobile Payments in Central and Eastern Europe – Information, Communications & Entertainment, KPMG Central and Eastern Europe Ltd., Budapest, Hungary, 2009.

http://kpmghu.lcc.ch/dbfetch/52616e646f6d4956ab2c5aaf8e0aab37eaab0d70d7a2fc 2c4ceec0b033411be5/cee_mobile_payments.pdf, Stand: 22.02.2010.

Agrawal (2009): Agrawal, Mohit: Mobile Money Transfer (MMT), Online-Artikel, publiziert am 28.05.2009, in: www.telecomcircle.com

http://www.telecomcircle.com/2009/05/mobile-money-transfer-mmt/, Stand: 11.01. 2010.

Alby (2008): Alby, Tom: Das mobile Web, Carl Hanser Verlag, München, 2008.

Andersson/Fischer-Hübner/Lundin (2003): Andersson, Christer; Fischer-Hübner, Simone; Lundin, Reine: mCrowds: Anonymity for the Mobile Internet. S. 79-92.

http://www.humanit.org/pdf/HumanIT_2003_Ch5_Andersson_et_al.pdf, Stand: 03. 01.2009.

Andersson/Lundin/Fischer-Hübner (2004): Andersson, Christer; Lundin, Reine; Fischer-Hübner, Simone: Privacy Enhanced WAP Browsing with mCrowds - Anonymity Properties and Performance Evaluation of the mCrowds System - Proceedings of the ISSA 2004 Conference, Johannesburg - Karlstad University, Sweden, Department of Computer Science.

http://icsa.cs.up.ac.za/issa/2004/Proceedings/Full/046.pdf, Stand: 03.01.2009.

Andreoli (2008): Andreoli, Giorgio: Mobile payments - reloaded, in: Ericsson Business Review, Issue no 3, 2008.

http://www.ericsson.com/ericsson/corpinfo/publications/index.shtml, Stand: 06.01. 2009.

Becker/Krcmar/Niehaves (2009): Becker, Jörg; Krcmar, Helmut; Niehaves, Björn (Hrsg.): Wissenschaftstheorie und gestaltungsorientierte Wirtschaftsinformatik, Physica-Verlag, Heidelberg, 2009.

Bender (2009): Bender, Hanno: Deutsche Bank bietet Mobile-Payment-Services, in: derhandel.de, Online-Artikel, publiziert am 12.03.2009.

http://www.derhandel.de/news/finanzen/pages/Deutsche-Bank-bietet-Mobile-Payme nt-Services_827.html, Stand: 17.02.2010.

Beutelspacher/Schwenk/Wolfenstetter (2006): Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus-D.: Moderne Verfahren der Kryptographie: Von RSA zu Zero-knowledge, 6. Auflage, Vieweg-Verlag/GWV-Fachverlage, Wiesbaden, 2006.

Beutelspacher (2007): Beutelspacher, Albrecht: Kryptologie: eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen, Verheimlichen, 8. aktualisierte Auflage, Vieweg-Verlag/GWV-Fachverlage, Wiesbaden, 2007.

Binder (2005): Binder, Markus: PKI - Public Key Infrastruktur, Ausarbeitung, Seminar „Internetsicherheit“, Technische Universität München, 2005.

http://www2.net.informatik.tu-muenchen.de/teaching/WS05/security/ausarbeitungen/ 04-Markus_Binder-PKI.pdf, Status: 25.02.2010.

Bizer/Spiekermann/Günther (2006): Bizer, Johann; Spiekermann, Sarah; Günther, Oliver [u. a.]: TAUCIS-Technikfolgen-Abschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung, 1. Auflage, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel und Institut für Wirtschaftsinformatik an der Humboldt-Universität in Berlin, 2006.

http://www.taucis.hu-berlin.de/_download/TAUCIS_Studie.pdf, Stand: 27.02.2010.

Bertsch (2001): Bertsch, Andreas: Digitale Signaturen, Springer-Verlag, Berlin, Heidelberg, 2001.

Best (2008): Best, Joe: Around the world in NFC and contactless payments, in: www.zdnet.com.au, Online-Artikel, publiziert am 18.01.2008.

http://www.zdnet.com.au/news/communications/soa/Around-the-world-in-NFC-and-contactless-payments/0,130061791,339285175,00.htm, Stand: 19.02.2010.

Borchers (2003): Borchers, Detlef: Handy als Portemonnaie - Bezahlen mit dem Telefon ist Zukunftsmusik, in: www.nzz.ch, Online-Artikel, publiziert am 04.07.2003.

http://www.nzz.ch/2003/07/04/em/article8YE1P.html, Stand: 07.02.2010.

Bös (2010): Bös, Nadine: Ziegen statt Geld für die Verwandten in Afrika, in: faz.net, Frankfurter Allgemeine Zeitung, Online-Artikel, publiziert am 21.02.2010.

http://www.faz.net/s/RubE2C6E0BCC2F04DD787CDC274993E94C1/Doc~EBCCDB999683346A8A56AB2800E07206A~ATpl~Ecommon~Scontent.html, Stand: 21.02.2010.

Brinker/Scholz (2007): Brinker, Ulrich; Scholz, Heike (Hrsg.): Mobile Quality - Your Marketing Information Service, Ausgabe 9, in: pressetext, www.pte.at, publiziert am 10.05.2007.

http://img.pte.at/files/binary/3075.pdf, Stand: 24.02.2010.

Brown (2006): Brown, Andrew: They know all about you, in: The Guardian, Online-Artikel, publiziert am 28. August 2006.

http://www.guardian.co.uk/world/2006/aug/28/usa.searchengines, Stand: 27.10.2009.

BSI (2001): Das Ende der Anonymität? Datenspuren in modernen Netzen, Online-Publikation der Studie "Das Ende der Anonymität? Datenspuren in modernen Netzen", Bundesamt für Sicherheit in der Informationstechnik–BSI, Bonn und SecuMedia Verlags-GmbH, Ingelheim, 2001, in: www.bsi.bund.de

https://www.bsi.bund.de/cln_165/ContentBSI/Publikationen/Studien/anonym/wasistanonymitaet.html, Stand: 20.06.2009.

BSI (2004): Risiken und Chancen des Einsatzes von RFID-Systemen - Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit. Bundesamt für Sicherheit in der Informationstechnik–BSI, Bonn und SecuMedia Verlags-GmbH, Ingelheim, 2004.

http://www.bsi.bund.de/fachthem/rfid/RIKCHA.pdf, Stand: 31.01.2009.

BSI (2006): Pervasive Computing: Entwicklungen und Auswirkungen, Bundesamt für Sicherheit in der Informationstechnik–BSI, Bonn und SecuMedia Verlags-GmbH, Ingelheim, 2006.

http://www.bsi.bund.de/literat/studien/percenta/Percenta_bfd.pdf, Stand: 01.06.2009.

BSI (2007): Der „Leitfaden IT-Sicherheit“ – Info-Broschüre von Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2007.

http://www.bsi.bund.de/gshb, Stand: 15.10.2008.

Bulander/Schiefer/Decker (2005): Bulander, Rebecca; Schiefer, Gunther; Decker, Michael: Anonymity by Design – Eine Architektur zur Gewährleistung von Kundenschutz im mobilen Marketing. In: Hampe, J. F.; Lehner, F.; Pousttchi, K.; Rannenberg, K.; Turowski, K.: (Hrsg.): Mobile Business – Processes, Platforms, Payments. Proceedings zur 5. Konferenz Mobile Commerce Technologien und Anwendungen (MCTA 2005). Bonn, 2005. (S. 87 - 100).

http://www.aifb.kit.edu/images/4/4f/2005_821_Bulander_Anonymity_by_De_1.pdf, Stand: 27.10.2009.

Butcher (2008): Butcher, Dan: GSMA calls for Pay-Buy-Mobile handsets, Online-Artikel, publiziert am 19.11.2008, in: Mobile Marketer

http://www.mobilemarketer.com/cms/news/associations/2134.html, Stand: 22.02.2010.

Carr (2007): Carr, Mahil: Mobile Payment Systems and Services: An Introduction, IDBRT, Hyderabad, India, 2007.

http://www.mpf.org.in/pdf/Mobile%20Payment%20Systems%20and%20Services.pdf, Stand: 12.01.2009.

Chaum (1981): Chaum, David: Ultraceable Electronic Mail, Return Addresses and Digital Pseudonyms, Communications of the ACM, Vol. 24, No. 2, 1981, S. 84-88.

http://www.freehaven.net/anonbib/cache/chaum-mix.pdf, Stand: 04.01.2009.

Chmielewicz (1994): Chmielewicz, Klaus: Forschungskonzeptionen der Wirschaftswissenschaft, Schäffer-Poeschel, Stuttgart, 1994.

Choi et al. (2007): Choi, Seung H.; Collins, David; Ure, John; Lovelock, Peter: Mobile Payments in Asia Pacific – Information, Communications & Entertainment, KPMG 2007.

http://www.kpmg.ca/en/industries/ice/MobileAsia.html, Stand: 19.12.2009.

Clark (2009): Clark, Sarah: French banks, network operators publish Payez Mobile specifications, Online-Artikel, in: nearfieldcommunicationsworld.com, publiziert am 28.05.2009.

http://www.nearfieldcommunicationsworld.com/2009/05/28/31208/french-banks-network-operators-publish-payez-mobile-specifications/, Stand: 17.02.2010.

Cuche (2001): Cuche, Nicholas A.: Elektronisches Geld: Wirklichkeit und Fiktion, in: Die Volkswirtschaft - Das Magazin für Wirtschaftspolitik 4-2001.

http://www.seco.admin.ch/dokumentation/publikation/00007/00021/01612/index.html?lang=de, Stand: 23.05.2009.

Dadam (1996): Dadam, Peter: Verteilte Datenbanken und Client/Server-Systeme. Grundlagen, Konzepte, Realisierungsformen. Springer-Verlag, Heidelberg, 1996.

Dahlberg et al. (2006): Dahlberg, Tomi; Mallat, Niina; Ondrus, Jan; Zmijewska, Agnieszka: Mobile Payment Market and Research - Past, Present and Future, in: The Proceedings of the Helsinki Mobility Roundtable 2006, MRT'06. Helsinki (Finland) : Helsinki School of Economics, 2006.

http://project.hkkk.fi/helsinkimobility/papers/Mobile%20Applications_3_1.pdf, Stand: 13.11.2009.

Dahlberg et al. (2008): Dahlberg, Tomi; Mallat, Niina; Ondrus, Jan; Zmijewska, Agnieszka: Past, present and future of mobile payments research - A literature review, *Electronic Commerce Research and Applications*, Jul. 2008, Vol. 7, Issue 2, p. 165-181.

http://www.janondrus.com/wp-content/uploads/2008/05/ecra2007-inpress.pdf, Stand: 13.11.2009.

Dannenberg/Ulrich (2004): Dannenberg, Marius; Ulrich, Anja: E-payment und E-billing: Elektronische Bezahlsysteme für Mobilfunk und Internet, Gabler Verlag, 2004.

De Laive (2009a): De Laive, Patrick: The Social Networking revolution is just getting started. There's so much more to come. Online-Artikel, publiziert am 17.08.2009, in: thenextweb.com.

http://thenextweb.com/2009/08/17/beginning-social-network-revolutio/, Stand: 17.02.2010.

De Laive (2009b): De Laive, Patrick: World's First: Social Network to Launch Mobile Payments. Online-Artikel, publiziert am 18.09.2009, in: thenextweb.com.

http://thenextweb.com/2009/09/18/social-network-to-launch-mobile-payments/, Stand: 17.02.2010.

Deloitte & Touche LLP (2008): Contactless payments technology-Catching the new wave, London, UK, 2008.

http://www.deloitte.com/assets/Dcom-UnitedKingdom/Local%20Assets/Documents/UK_FS_ContactlessPaymentsTechnology(4).pdf, Stand: 18.09.2009.

Demuth/Rieke (1998): Demuth, Thomas; Rieke, Andreas: Anonym im World Wide Web? JANUS - Schutz von Inhalteanbietern im WWW, In: Datenschutz und Datensicherheit (DuD), Jahrgang 22, Ausgabe 11, S. 623-627.

http://www.demuth.biz/veroeffentlichungen/dud98.pdf, Stand: 21.06.2009.

Dialogic (2008): USSD Services for Interactive Mobile Users, Application Note, Dialogic Corporation, Montreal, Quebec, Canada, 2008.

http://www.dialogic.com/products/docs/appnotes/11038_USSD_an.pdf, Stand: 03. 01.2009.

Dulz (2005): Dulz, Winfried: WAP (Wireless Application Protocol), Online-Artikel, in: Informatiklexikon, www.gi-ev.de, Gesellschaft für Informatik e.V., Institut für Informatik, Universität Erlangen, 2005.

http://www.gi-ev.de/no_cache/service/informatiklexikon/informatiklexikon-detailansicht/meldung/wap-wireless-application-protocol-91.html, Stand: 28.01.2010.

Durix (2004): Durix, Jean-François: Mobile Proximity Services - Bringing the best of physical & mobile worlds to end-users, Whitepaper, Gemplus, 2004.

http://www.gemplus.com/pss/telecom/download/Mobile_proximity_services_whitepaper_2004.pdf, Stand: 02.10.2009.

ECB Report (2004): E-Payments without frontiers – Issues paper for the ECB Conference on 10 November 2004.

http://www.ecb.int/pub/pdf/other/epaymentsconference-issues2004en.pdf, Stand: 12.01.2010.

Emmert (2006): Emmert, Monika: Grundrechtsverträgliche DRM-Systeme gesucht, in: heise online, Online-Artikel, publiziert am 05.05.2006.

http://www.heise.de/newsticker/meldung/Grundrechtsvertraegliche-DRM-Systeme-gesucht-122241.html, Stand: 07.02.2010.

Enzmann/Eckert (2002): Enzmann, Matthias; Eckert, Claudia: Pseudonymes Einkaufen physischer Güter, in: Horster, P. (Hrsg.): Sichere Geschäftsprozesse, S. 55 ff., 2002, Arbeitskonferenz Elektronische Geschäftsprozesse mit Schwerpunkt IT-Sicherheit, IT-Verlag für Informationstechnik GmbH, Höhenkirchen, 2002.

http://private.sit.fraunhofer.de/~enzmann/papers/ebp2002.pdf, Stand: 01.02.2010.

Ernestus et al. (1997): Ernestus, Walter; Ermer, Dieter J.; Hube, Martin; Köhntopp, Marit; Knorr, Michael; Quiring-Kock, Gisela; Schläger, Uwe; Schulz, Gabriel: Datenschutzfreundliche Technologien-Arbeitspapier. Arbeitsgruppe “Datenschutzfreund-

liche Technologien” des Arbeitskreises “Technische und organisatorische Datenschutzfragen” der Datenschutzbeauftragten des Bundes und der Länder, 1997.

http://www.datenschutz-bayern.de/technik/grundsatz/apdsft.htm, Stand: 26.10.2009.

European Communities (2002): Digital Content for Global Mobile Services - Executive Summary, Commission of the European Communities, Directorate-General for the Information Society, Office for Official Publications of the European Communities, Luxembourg, 2002.

ftp://ftp.cordis.europa.eu/pub/econtent/docs/mobilestudy_es_en.pdf, Stand: 11.10. 2009.

Ezell (2009): Ezell, Stephen: Explaining International IT Application Leadership: Contactless Mobile Payments, Information Technology and Innovation Foundation (ITIF), Washington, DC, USA, 2009.

http://www.itif.org/files/2009-mobile-payments.pdf, Stand: 13.02.2010.

Federrath et al. (1997): Federrath, Hannes; Jerichow, Anja; Kesdogan, Dogan; Pfitzmann, Andreas; Spaniol, Otto: Mobilkommunikation ohne Bewegungsprofile, in: Günter Müller, Andreas Pfitzmann (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik, Addison-Wesley-Longman, 1997, S. 169-180.

http://www-sec.uni-regensburg.de/publ/1997/FJKP1_97BuchMobil.pdf, Stand: 30.01. 2010.

Federrath/Martius (1998): Federrath, Hannes; Martius, Kai: Anonymität und Authentizität im World Wide Web. ITG-Fachbericht 153, Vorträge der ITG-Fachtagung 'Internet - frischer Wind in der Telekommunikation', VDE-Verlag, Stuttgart, 1998, S. 91-101.

http://epub.uni-regensburg.de/7396/1/FeMa1_98ITG.pdf, Stand: 30.10.2009.

Federrath/Pfitzmann (1998): Federrath, Hannes; Pfitzmann, Andreas: „Neue“ Anonymitätstechniken - Eine vergleichende Übersicht, in: Datenschutz und Datensicherheit, 22/11 (1998), S. 628-632.

http://www.semper.org/sirene/publ/FePf2_98.pdf, Stand: 30.10.2009.

Federrath (2003): Federrath, Hannes: Das AN.ON-System: Starke Anonymität und Unbeobachtbarkeit im Internet. in: Helmut Bäumler, Albert von Mutius (Hrsg.): Anonymität im Internet - Grundlagen, Methoden und Tools zur Realisierung eines Grundrechts, Verlag Vieweg, 2003, S. 172-178.

http://epub.uni-regensburg.de/7351/1/FederrathSoAk2002.pdf, Stand: 30.10.2009.

Federrath (2006): Federrath, Hannes: Anonymität.Online, Technik-Szenarien-Geschäftsmodelle, Technische Ergebnisse, Präsentationsunterlagen, Technik-Szenarien-Geschäftsmodelle, Abschlussveranstaltung des BMWi-Projektes „Starke Anonymität und Unbeobachtbarkeit im Internet“ 24.11.2006, BMWi, Berlin.

http://anon.inf.tu-dresden.de/bmwi2006/Federrath2006-11-24BMWiANON.pdf, Stand: 05.02.2010.

Fischer/Keil-Slawik/Richter (2001): Fischer, Carsten; Keil-Slawik, Reeinhard; Richter, Andreas: Verhaltensprofile im Internet, in: Keil-Slawik, Reinhard (Hrsg.): Digitale Medien und gesellschaftliche Entwicklung: Arbeit, Recht und Gemeinschaft in der Informationsgesellschaft, Münster [u. a.], Waxmann-Verlag, 2001, S. 65-81.

Florl (2001): Florl, Meyke: Aufgaben in Call Centern, in: Rabbe, Georg; Jahnke, Jennifer (Hrsg.): Praxishandbuch Call Center, 1. Auflage, Ecmc Gernot Gehrke-Verlag, Marl, 2001.

Fox/Horster/Kraaibeek (1995): Fox, Dirk; Horster, Patrick; Kraaibeek, Peter: Grundüberlegungen zu Trust Centern, In: Horster, P. (Hrsg.): Trust Center. Proceedings der Arbeitskonferenz Trust Center 95, Vieweg-Verlag, Braunschweig 1995, S. 1-10.

http://www.secorvo.de/publikationen/trustcen.pdf, Stand: 25.08.2010.

Fröming/Gronau/Aethner (2007): Fröming, Jane; Gronau, Norbert; Aethner, Christian: Innovativer Groupwareeinsatz in Lehre und Forschung, in: Laabs, Hans-Joachim (Hrsg.): MultimeDies 2007-Wir gehen multimedial: kommt Ihr mit? Universitätsverlag Potsdam, Universität Potsdam, 2007, S. 109-115.

Gajek (2009): Gajek, Henning: Bezahldienst Luupay hört in Deutschland auf, in: teltarif.de, Pressemitteilung, publiziert am 10.03.2009

http://www.teltarif.de/luupay-stellt-bezahldienst-ein/news/33417.html, Stand: 18.10. 2010.

Garstka (2003): Garstka, Hansjürgen: Informationelle Selbstbestimmung und Datenschutz - Das Recht auf Privatsphäre, in: Schulzki-Haddouti, C. (Hrsg.), Bürgerrechte im Netz, Leske+Budrich-Verlag, 2003, S. 48-70.

http://www.bpb.de/files/YRPN3Y.pdf, Stand: 27.02.2010.

Gartner (2007): Gartner Says Mobile Messages to Surpass 2 Trillion Messages in Major Markets in 2008. Pressemitteilung, Gartner, Inc., STAMFORD, Conn., USA, December 17, 2007.

http://www.gartner.com/it/page.jsp?id=565124, Stand: 28.01.2010.

Gartner (2008): Gartner Says Worldwide Mobile Payment Users to Total 33 Million in 2008. Pressemitteilung, Gartner, Inc., STAMFORD, Conn., USA, April 21, 2008.

http://www.gartner.com/it/page.jsp?id=652308, Stand: 28.01.2010.

Gartner (2009a): Gartner Says Number of Mobile Payment Users Worldwide to Increase 70 Percent in 2009. Pressemitteilung, Gartner, Inc., STAMFORD, Conn., USA, May 28, 2009.

http://www.gartner.com/it/page.jsp?id=995812, Stand: 12.01.2010.

Gartner (2009b): Gartner Identifies the Top 10 Consumer Mobile Applications for 2012. Pressemitteilung, Gartner, Inc., STAMFORD, Conn., USA, November 18, 2009.

http://www.gartner.com/it/page.jsp?id=1230413, Stand: 12.01.2010.

Goldhammer (2009): Goldhammer, Klaus: Das Handy ist die Geldbörse von morgen. Mobile Payment schon jetzt Alltag in Japan, Online-Artikel, publiziert am 27.08.2009, in: GOLDMEDIA Blog.

http://www.goldmedia.com/blog/2009/08/das-handy-ist-die-geldborse-von-morgen-mobile-payment-schon-jetzt-alltag-in-japan/, Stand: 22.02.2010.

Goltzsch (2003): Goltzsch, Patrick: Anonymität im Internet - Die technische Verteidigung eines Grundrechtes, Bundeszentrale für Politische Bildung, Schriftenreihe Bd. 382, 2003, S. 109-126.

http://www.bpb.de/files/D9AWDO.pdf, Stand: 04.07.2009.

Gottschalk (2008): Gottschalk, Anne: Anruf statt Parkschein, in: heise online, News, 2008.

http://www.heise.de/newsticker/meldung/Anruf-statt-Parkschein-194915.html, Stand: 21.02.2010.

Gourley et al. (2002): Gourley, David; Totty, Brian; Sayer, Marjorie; Reddy, Sailu; Aggarwal, Anshu: HTTP: the definitive guide, 1. Edition, Verlag O'Reilly Media, Inc., Sebastopol, CA, USA 2002.

Graf (2008): Graf, Daniela (Redaktion): Mobile Marketing - Mobile CRM, Schriftenreihe Marketing & Vertrieb, Band 3, Hrsg. BITKOM - Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., www.bitkom.org, Berlin, 2008.

http://www.bitkom.org/files/documents/Mobile_Marketing.pdf, Stand: 20.02.2010.

Grimm/Lohndorf/Scholz (1999): Grimm, Rudiger; Lohndorf, Nils; Scholz Philip: Datenschutz in Telediensten (DASIT) am Beispiel von Einkaufen und Bezahlen im Internet, in: Datenschutz und Datensicherheit, 23/5, (1999), S. 272-277.

http://www.uni-kassel.de/fb7/oeff_recht/publikationen/pubOrdner/DuD_DASIT5.pdf, Stand: 01.02.2010.

Haglmüller (2009): Haglmüller, Manuel: Afrika: Gelddienste liefern Mobilfunkern Milliarden, in: pressetext.de, Online-Artikel, publiziert am 21.07.2009.

http://pressetext.de/news/090721031/,Stand: 15.02.2010.

Hansen/Meissner (2007): Hansen, Marit (Editor); Meissner, Sebastion (Editor) [u. a.]: Verkettung digitaler Identitäten - Untersuchung im Auftrag des Bundesministeriums für Bildung und Forschung, Verleger: Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel, 2007.

https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf, Stand: 31.05.2009.

Hansen/Neumann (2009): Hansen, Hans R.; Neumann, Gustaf: Wirtschaftsinformatik 1 - Grundlagen und Anwendungen, 10. völlig neu bearbeitete und erweiterte Auflage, Lucius & Lucius Verlagsgesellschaft, Stuttgart 2009.

Harnick (2009): Harnick, Chris: Facebook looking into mobile payments, in: Mobile Marketer, Online-Artikel, publiziert am 01.09.2009.

http://www.mobilemarketer.com/cms/news/social-networks/4071.html, Stand: 17.02.2010.

Heikkinen (2009): Heikkinen, Päivi: A framework for evaluating mobile payments, Bank of Finland, BoF Online 2/2009, 2009.

http://www.bof.fi/NR/rdonlyres/DE4FC809-A68B-428A-A912-020DB010F53A/0/BoF_Online_2_2009.pdf, Stand: 25.07.2009.

Henkel (2001): Henkel, Joachim: Anforderungen an Zahlungsverfahren im E-Commerce, In: Teichmann, Rene; Nonnenmacher, Martin; Henkel, Joachim: E-Commerce und E-Payment: Rahmenbedingungen, Infrastruktur, Perspektiven. Gabler-Verlag, Wiesbaden, 2001, S. 103-120.

http://www.wim.uni-koeln.de/fileadmin/alt/lehre/ss2004/Electronic_Business/Anf_E-Paym_2001.pdf, Stand: 24.05.2009.

Henkel (2002): Henkel, Joachim: Mobile Payment. In: Silberer, Günter; Wohlfahrt, Jens; Wilhelm, Thorsten (Hrsg.): Mobile Commerce, Gabler-Verlag, Wiesbaden, 2002.

http://www.en.inno-tec.bwl.uni-muenchen.de/research/proj/abgeschlossen/innozahlverfahren/henkel1.pdf, Stand: 24.05.2009.

Hess et al. (2005): Hess, Thomas; Hagenhoff, Svenja; Hogrefe, Dieter; Linnhoff-Popien, Claudia; Rannenberg, Kai; Straube, Frank (Hrsg.): Mobile Anwendungen - best practices in der TIME-Branche - Sieben erfolgsreiche Geschäftskonzepte für mobile Anwendungen, Göttingen, 2005.

http://webdoc.sub.gwdg.de/univerlag/2006/mobiledienste_book.pdf, Stand: 28.01. 2009.

Hesselbach (2009): Hesselbach, Martin: Android - Revolutioniert Google die Handywelt? Knol-Artikel, Version: 89, 24.05.2009.

http://knol.google.com/k/android#9%282E%29_Android_und_Datenschutz%283F%29, Stand. 07.02.2010.

Heuer/Ulmer (2006): Heuer, Jörg; Ulmer, Claus D.: Datenschutz und Anonymisierungsverfahren, Präsentationsunterlagen, Technik-Szenarien-Geschäftsmodelle, Abschlussveranstaltung des BMWi-Projektes „Starke Anonymität und Unbeobachtbarkeit im Internet“ 24.11.2006, BMWi, Berlin.

http://anon.inf.tu-dresden.de/bmwi2006/Ulmer2006-11-24BMWIANON.pdf, Stand: 05.02.2010.

Himmelspach et al. (1996): Himmelspach, Andrea; Runge, Alexander; Schubert, Petra; Zimmermann, Hans D.: Anforderungen an elektronische Zahlungssysteme, Arbeitsbericht Business Media Nr. 51, Institut für Wirtschaftinformatik, Universität St. Gallen, Schweiz, 1996.

http://www.hsw-basel.ch/iwi/publications.nsf/id/41, Stand: 20.05.2009.

Hoeren (2009): Hoeren, Thomas: Internetrecht. Skriptum, Institut für Informations-, Telekommunikations- und Medienrecht, Universität Münster, März 2009.

http://www.uni-muenster.de/Jura.itm/hoeren/materialien/Skript/Skript_Maerz2009.pdf, Stand: 08.11.2009.

Hong/Kong/Gerla (2006): Hong, Xiaoyan; Kong, Jiejun; Gerla, Mario: "Mobility changes anonymity: new passive threats in mobile ad hoc networks" (2006). UC Los Angeles, Wireless Communications & Mobile Computing. 6 (3), S. 281-293.

http://portal.acm.org/citation.cfm?id=1133160 und http://repositories.cdlib.org/postprints/2041/, Stand: 24.06.2009.

Hu/Lee/Kou (2005): Hu, Wen-Chen; Lee, Chung-wei; Kou, Weidong: Advances in Security and Payment Methods for Mobile Commerce, Idea Group Publishing, Hershey, London, 2005.

IBM (2008): IBM Mobile Point-of-Sale solution, IBM Corporation, New York, USA, 2008.

Initiative D21 (2006): Mobile Bürgerdienste- Standard-Rahmenbedingungen für Mobile Bürgerdienste am Beispiel Mobiles Parken, Informationsbroschüre, Herausgegeben von Initiative D21 e.V., Berlin, 2006.

http://old.initiatived21.de/fileadmin/files/66_1163409498.pdf, Stand: 21.02.2010.

Illik (2002): Illik, Johann A.: Electronic Commerce: Grundlagen und Technik für die Erschließung elektronischer Märkte, 2. überarbeitete Auflage, Oldenbourg Wissenschaftsverlag, München, Wien, 2002.

JAP (2001): Technischer Hintergrund von JAP, Projekt: AN.ON - Anonymität.Online, Institut für Wirtschaftsinformatik, Universität Regensburg und Institut für Systemarchitektur, Technische Universität Dresden, 2001.

http://anon.inf.tu-dresden.de/JAPTechBgPaper.pdf, Stand: 07.01.2009.

Jain/Seri/Srinivasan (2008): Jain, Anchal; Seri, Sai Prasad, Srinivasan, Vikram: Mobile Payments: Sustainability of business models, in: FINsights - Technology Insights for the Financial Services Industry- Enterprise payments, Infosys Technologies Limited, Bangalore, India, 2008.

http://www.infosys.com/finsights/Documents/pdf/issue3/FINsights-Chp2.pdf, Stand: 15.07.2009.

Jones (2008): Jones, Chris: Payments Innovation - Mobile Payments – Präsentation in Payments Council Conference am 23. Januar 2008, PSE Consulting,

http://www.paymentscouncil.org.uk/events/, Stand: 10.01.2009.

Karnouskos/Hoepner/Holzmann-Kaiser (2003): „Globale Mobile Zahlungsdienste: Vision und Realität“, Karnouskos, Stamatis; Hoepner, Petra; Holzmann-Kaiser, Uwe; ONLINE 2003, 26. Europäische Congressmesse der IT- und TK Branche, Düsseldorf, 23 - 26 Sept. 2003.

Karnouskos (2004): Karnouskos, Stamatis: Mobile Payment: A journey through existing procedures and standardization initiatives, in: IEEE Communications Surveys & Tutorials, Volume 6, No. 4, 4th Quarter 2004.

http://www.comsoc.org/livepubs/surveys/public/2004/oct/pdf/KARNOUSKOS.pdf, Stand: 29.06.2009.

Keil-Slawik (2001): Keil-Slawik, Reinhard (Hrsg.): Digitale Medien und gesellschaftliche Entwicklung: Arbeit, Recht und Gemeinschaft in der Informationsgesellschaft, Münster [u. a.], Waxmann-Verlag, 2001.

Keles (2006): Keles, Fatih: Privacy in Location-based Services, Ausarbeitung Anwendungen 1 (AI), Fakultät Technik und Informatik, Hochschule für Angewandte Wissenschaften Hamburg, 2006.

http://users.informatik.haw-hamburg.de/~ubicomp/projekte/master2006/keles/abstract.pdf, Stand: 14.02.2010.

Keller/Meier/Schumacher (2002): Keller, Philipp; Meier, Martin; Schumacher, Raphael: Non-Repudiation in Electronic Transactions, Seminar: Internet Economics, Vortrag Nr. 2, Eidgenössische Technische Hochschule Zürich, Schweiz, 2002.

ftp://ftp.tik.ee.ethz.ch/pub/lehre/inteco/SS02/V2.PDF, Stand: 28.02.2010.

Kharif (2006): Kharif, Olga: Social Networking Goes Mobile, in: BusinessWeek.com Online-Artikel, publiziert am 31.05.2006.

http://www.businessweek.com/technology/content/may2006/tc20060530_170086.htm, Stand: 18.09.2009.

Khodawandi/Pousttchi/Wiedemann (2003): Khodawandi, D.; Pousttchi, K.; Wiedemann, D. G.: Akzeptanz mobiler Bezahlverfahren in Deutschland. In: Pousttchi, K.; Turowski, K. (Hrsg.): Mobile Commerce - Anwendungen und Perspektiven. Proceedings zum 3. Workshop Mobile Commerce. Augsburg, 2003. Gesellschaft für Informatik LNI P-25, Köllen Druck+Verlag, Bonn, 2003.

http://wi2.wiwi.uni-augsburg.de/pics/mobile/Uni-Augsburg_WI2-MC_MP-06-13.pdf, Stand: 26.05.2009.

Koch (2005): Koch, Frank A.: Internet-Recht: Praxishandbuch zu Dienstenutzung, Verträgen, Rechtsschutz, Wettbewerb, Haftung, Arbeitsrecht und Datenschutz im Internet, zu Links, Peer to Peer-Netzen und Domain-Recht, mit Musterverträgen, Oldenbourg-Wissenschaftsverlag, München, 2005.

Kobsa/Schreck (2003): Kobsa, Alfred; Schreck, Jörg: Privacy through pseudonymity in user-adaptive systems. ACM Transactions on Internet Technology Volume 3, Issue 2, New York, NY, USA, 2003, S. 149-183.

http://www.ics.uci.edu/~kobsa/papers/2003-TOIT-kobsa.pdf, Stand: 18.10.2009.

Köpsell/Federrath/Hansen (2003): Köpsell, Stefan; Federrath, Hannes; Hansen, Marit: Erfahrungen mit dem Betrieb eines Anonymiserungsdienstes, in: Datenschutz und Datensicherheit DuD 27/3 (2003), S. 139-142.

http://epub.uni-regensburg.de/7354/1/KoFHDuD2003.pdf, Stand: 30.10.2009.

Köpsell/Miosga (2005): Köpsell, Stefan; Miosga, Tobias: Strafverfolgung trotz Anonymität - Rechtliche Rahmenbedingungen und technische Umsetzung, in: Datenschutz und Datensicherheit 29 / 2005, S. 403 - 409. Vieweg Verlag. 2005.

http://eldorado.tu-dortmund.de:8080/bitstream/2003/22830/1/KoepsellPaper.pdf, Stand: 14.07.2009.

Köpsell/Pfitzmann (2003): Köpsell, Stefan; Pfitzmann, Andreas: Wie viel Anonymität verträgt unsere Gesellschaft? in: Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): Security, E-Learning, E-Services; 17. DFN-Arbeitstagung über Kommunikationsnetze, Düsseldorf, GI-Edition Lecture Notes in Informatics (LNI) P-44, Bonn 2003, S. 13-26.

http://dud.inf.tu-dresden.de/literatur/KoePf_03.pdf, Stand: 16.10.2009.

Kretschmann (2007): Kretschmann, Thomas: Anbieter denken um: Websuche wird anonym, Online-Artikel, publiziert am 24.07.2007.

http://www.tomshardware.com/de/Ask.com-Microsoft-Suchmaschine-Privacy,news-239670.html, Stand: 28.10.2009.

Krohn (2009): Krohn, Frederike: Mobile Banking & Mobile Payment: Zukunftsträchtig oder zum Scheitern verurteilt? in: Unternehmer.de, Online-Artikel, publiziert am 14.07.2009.

http://www.unternehmer.de/mobile-banking-mobile-payment-zukunftstraechtig-oder-zum-scheitern-verurteilt-744, Stand: 23.02.2010.

Kühling/Sivridis/Seidel (2008): Kühling, Jürgen; Sivridis, Anastasios; Seidel, Christian (2008): Datenschutzrecht, 1. Auflage, Verlag UTB, Stuttgart, 2008.

Laabs (2007): Laabs, Hans-Joachim (Hrsg.): MultimeDies 2007-Wir gehen multimedial: kommt Ihr mit? Universitätsverlag Potsdam, Universität Potsdam, 2007.

Larson (2008): Larson, James A.: The Evolution of IVR Systems, Online-Artikel, publiziert am 01.06.2008.

http://www.speechtechmag.com/Articles/Column/Forward-Thinking/The-Evolution-of-IVR-Systems-49342.aspx, Stand: 14.03.09.

Lee/Hu/Kou (2007): Lee, Chung-wei; Hu, Wen-Chen; Kou, Weidong: Mobile commerce security and payment methods, in: Becker, Annie: Electronic commerce: concepts, methodologies, tools and applications, Ausg. 1, Florida Institute of Technology, Idea Group Inc., USA, 2007, S. 292-306.

http://www.idea-group.com/downloads/excerpts/01%20Hu.pdf, Stand: 14.08.2009.

Link (2003a): Link, Jörg: Mobile Commerce – Gewinnpotenziale einer stillen Revolution. Springer, Berlin – Heidelberg, 2003.

Link (2003b): Link, Jörg: M-Commerce: Die stille Revolution bis zum Electronic Aided Acting, in: Link, Jörg: Mobile Commerce – Gewinnpotenziale einer stillen Revolution. Springer, Berlin – Heidelberg, 2003, S. 1-39.

Logara (2007): Logara, Tomislav: Mobile Business im B2C: Komplexität als Ursache von Produktivitätsengpässen in den Distributionskanälen des deutschen B2C-Marktes, 2. Auflage, Books on Demand-Verlag, Norderstedt, 2007.

Maffeis (1997): Maffeis, Silvano: Client/Server Term Definition, in: Encyclopedia of Computer Science, Hemmendinger, D.; Ralston, A.; Reilly, E. D., eds. International Thomson Computer Publishing, 1998.

http://www.maffeis.com/articles/research/client_server.pdf, Stand: 29.01.2010.

Martellaro (2010): Martellaro, John: iPhone, Android Gaining Market Share, Microsoft, Palm Losing, Online-Artikel, publziert am 10.02.2010, in: the Mac Observer.

http://www.macobserver.com/tmo/article/iphone_android_gaining_market_share_microsoft_palm_losing/, Stand: 22.02.2010.

Matthiessen/Unterstein (2003): Matthiessen, Günter; Unterstein, Michael**:** Relationale Datenbanken und SQL, 3. aktualisierte Auflage, Addison-Wesley-Verlag, München, 2003.

McKitterick/Dowling (2003): McKitterick, David; Dowling, Jim: State of the Art Review of Mobile Payment Technology, Trinity College Dublin, Department of Computer Science, 2003.

https://www.cs.tcd.ie/publications/tech-reports/reports.03/TCD-CS-2003-24.pdf, Stand: 28.09.2009.

Meißner (2002): Meißner, Robert: Data Encryption Standard (DES) - Einführung - Funktionsweise - Risiken - Alternativen. Seminarunterlagen, Fakultät für Informatik, Technische Universität Chemnitz, 2002.

http://archiv.tu-chemnitz.de/pub/2002/0059/data/PS_Electronic_Banking.pdf, Stand: 31.01.2010.

Mielke (2002): Mielke, Bernd: Übertragungsstandards und –bandbreiten in der Mobilkommunikation, in: Silberer, G.; Wohlfahrt, J.; Wilhelm, T. (Hrsg.); Mobile Commerce: Grundlagen, Geschäftsmodelle, Erfolgsfaktoren, Gabler Verlag, Wiesbaden, 2002, S. 185-202.

MMA (2008): Mobile Marketing Industry Glossary, Mobile Marketing Association, New York, USA, 2008.

http://www.mmaglobal.com/glossary.pdf, Stand: 01.03.2010.

Mobey Forum (2003): Mobey Forum White Paper on Mobile Financial Services 1.1, White Paper, Mobey Forum Mobile Finacial Services Ltd., 2003.

http://www.mobeyforum.org/files/Mobey%20Forum%20White%20Paper%20on%20Mobile%20Financial%20Services%20v1_14.pdf, Stand: 13.01.2010.

Moos (2004): Moos, Alfred: Datenbank-engineering: Analyse, Entwurf und Implementierung objektrelationaler Datenbanken, mit UML, DB2-SQL und Java, 3. Auflage, Vieweg-Verlag/GWV-Fachverlage, Wiesbaden, 2004.

Müller (2010a): Müller, Reinhard: Karlsruhe stoppt Vorratsdatenspeicherung - Merkel warnt vor einem „Vakuum“, in: FAZ, Frankfurter Allgemeine Zeitung GmbH, Online-Artikel, publiziert am 02.03.2010.

http://www.faz.net/s/Rub594835B672714A1DB1A121534F010EE1/Doc~EE7C259587FE84E7386196C3E7FECBC02~ATpl~Ecommon~Scontent.html, Stand: 03.03.2010.

Müller (2010b): Müller, Reinhard: Urteil zur Vorratsdatenspeicherung: Rückschlüsse bis in die Intimsphäre, in: FAZ, Frankfurter Allgemeine Zeitung GmbH, Online-Artikel, publiziert am 03.03.2010.

http://www.faz.net/s/RubD5CB2DA481C04D05AA471FA88471AEF0/Doc~E1244C3DFB7C348FCA5E7608CC1EE5B08~ATpl~Ecommon~Scontent.html, Stand: 03.03.2010.

Müller-Jung (2010): Müller-Jung, Joachim: Wegweisend: Die Kartographie der Datenspione, in: FAZ, Frankfurter Allgemeine Zeitung GmbH, Online-Artikel, publiziert am 19.02.2010.

http://www.faz.net/s/Rub163D8A6908014952B0FB3DB178F372D4/Doc~E987C36549B6A4F72B2523777C8692102~ATpl~Ecommon~Scontent.html, Stand: 19.02.2010.

Neuhaus (2003): Neuhaus, Daniel: Mobile Ticketing-Killerapplikation in der mobilen Welt, in: Kruse, Jörn (Hrsg.): MultiMedia Mobil, Verlag-Reinhard Fischer, München, 2003, S. 97-108.

Ohland (2009): Ohland, Günther: Knipsen statt Tippen mit mobilen Handy-Codes, in: www.teltarif.de, Online-Artikel, publiziert am 03.01.2009.

http://www.teltarif.de/arch/2009/kw01/s32493.html, Stand: 19.02.2010.

Ondrus/Pigneur (2006): Ondrus, Jan; Pigneur, Yves: A Multi-Stakeholder Multi-Criteria Assessment Framework of Mobile Payments: An Illustration with the Swiss Public Transportation Industry. Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06) Track 2, Kauai, Hawaii, 2006.

http://www2.computer.org/portal/web/csdl/doi/10.1109/HICSS.2006.21, Stand: 11. 10.2009.

O'Reilly/Milstein/Lang (2009): O'Reilly, Tim; Milstein, Sarah; Lang, Jörgen W. (Übersetzer): Das Twitter-Buch, 1. Auflage, O'Reilly Media, Inc. Sebastopol, CA, USA, 2009.

o. V. (2002): Illegaler Handel mit Email-Adressen blüht, publiziert am 14.05.2002, in: CHIP Online, http://www.chip.de/news/Illegaler-Handel-mit-E-Mail-Adressen-blueht_34204608.html, Stand: 28.10.2009.

o. V. (2007a): Der gläserne Netznutzer - Motivation zur Nutzung von Anonymisierungsdiensten, publiziert in Oktober 2006, aktualisiert in April 2007, in: Tariftipp, http://www.tariftip.de/rubrik2/19440/Der-glaeserne-Netznutzer-Motivation-zur-Nutzung-von-Anonymisierungsdiensten.html, Stand: 28.10.2009.

o. V. (2007b): Mobile Ticketing: Innovative paperless ticketing solutions, Präsentationsunterlagen, MessageNet, Melbourne, Australia, 2007.

http://www.messagenet.com.au/PR%5CFRE_MobileTicketing_D03.pdf, Stand: 20. 02.2010.

o. V. (2009a): Die aktuelle Situation, Online-Artikel, in: gulli, publiziert am 13.10. 2009.

http://www.gulli.com/entertainment/internet/internet-gegenwart, Stand: 28.10.2009.

o. V. (2009b): Mobile Payment: Mit dem Handy bezahlen, Online-Artikel, in: FOCUS Online, publiziert am 31.05.2009.

http://www.focus.de/digital/handy/mobile-payment-mit-dem-handy-bezahlen_aid_403733.html, Stand: 02.03.2010.

o. V. (2010a): What is Point of Sale (POS)?, in: Posmatic, Online-Artikel, o. D.

http://www.posmatic.com/point-of-sale/what-is-point-of-sale.php, Stand: 13.02.2010.

o. V. (2010b): Sicherheitsproblematik, in: Virenschutz.info, Online-Artikel, o. D.

http://www.virenschutz.info/Sicherheitsproblematik-Wlan-Tutorials-9.html, Stand: 28.-02.2010.

o. V. (2010c): Mobile Payment: In Deutschland bisher ohne Erfolg, in: teltarif.de, Online-Artikel, o. D.

http://www.teltarif.de/i/mobile-payment.html, Stand: 02.03.2010.

o. V. (2010d): Vorratsdatenspeicherung: Unternehmen fordern Millionen von Regierung, in: FAZ, Frankfurter Allgemeine Zeitung GmbH, Online-Artikel, publiziert am 02.03.2010.

http://www.faz.net/s/RubCC801D08D34145F4A46F9638F4147CFF/Doc~E16470984BF1243EA914502360229C87E~ATpl~Ecommon~Scontent.html, Stand: 09.03.2010.

Palme/Berglund (2004): Palme, Jacob; Berglund, Mikael: Anonymity on the Internet, 2004.

http://people.dsv.su.se/~jpalme/society/anonymity.pdf, Stand: 28.06.2009.

Parlak (2009): Parlak, Deniz: Geschäftsmodelle im Mobile Business am Beispiel des M-Parking in Deutschland, Diplomarbeit, Institut für Wirtschaftsinformatik, Leibniz Universität Hannover, 2009.

http://www.iwi.uni-hannover.de/cms/images/stories/Diplomarbeiten/da_parlak.pdf, Stand: 21.02.2010.

Pfitzmann/Waidner (1986): Pfitzmann, Andreas; Waidner, Michael: Networks without user observability, in: EUROCRYPT 1985: 245-253 (Copyright Springer-Verlag, Heidelberg [u. a.], 1986).

http://dsns.csie.nctu.edu.tw/research/crypto/HTML/PDF/E85/245.PDF, Stand: 07.06.2009.

Pfitzmann (2006): Pfitzmann, Andreas: Abschlussvortrag Projekt AN.ON: Zukunftsskizze Anonymität im Netz, Präsentationsunterlagen, Abschlussveranstaltung des BMWi-Projektes „Starke Anonymität und Unbeobachtbarkeit im Internet“ 24.11.2006, BMWi, Berlin.

http://anon.inf.tu-dresden.de/bmwi2006/Pfitzmann2006-11-24BMWIANON.pdf, Stand: 05.02.2010.

Pfitzmann/Hansen (2009): Pfitzmann, Andreas; Hansen, Marit: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology, (Version v0.32, Dec. 18, 2009).

http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.32.pdf, Stand: 04.03. 2010.

Pleil (2003): Pleil, Thomas: Konvergenz der Konsortien - Aussichten für mobiles Bezahlen und M-Business, Eichstätt, Online-Artikel, publiziert in 2003.

http://www.kes.info/archiv/online/03-6-014.htm, Stand: 06.02.2010.

Pommerening (2007): Pommerening, Klaus: Kryptographische Protokolle - Pseudonyme, Vorlesungsmaterialien, letzte Änderung: 5. Juli 2007.

http://www.staff.uni-mainz.de/pommeren/DSVorlesung/KryptoProt/Pseudonyme.html, Stand: 27.10.2009.

Pößneck (2006): Pößneck, Lutz: IT der Zukunft - pervasiv und ubiquitär, Online-Artikel, in: Silicon.de, publiziert am 13.10.2006.

http://www.silicon.de/hardware/server-desktops/0,39038998,39178585,00/it+der+zukunft+pervasiv+und+ubiquitaer.htm, Stand: 27.02.2010.

Pousttchi/Selk/Turowski (2002): Pousttchi, Key; Selk, Bernhard; Turowski, Klaus: Akzeptanzkriterien für mobile Bezahlverfahren. In: Hampe, J. F.; Schwabe, G. (Hrsg.): Mobile and Collaborative Business 2002, Proceedings zur Teilkonferenz der Multikonferenz Wirtschaftsinformatik 2002, 10. September 2002, Nürnberg. Lecture Notes in Informatics (LNI) P-16. Gesellschaft für Informatik, Bonn 2002, S.51-67.

http://subs.emis.de/LNI/Proceedings/Proceedings16/GI-Proceedings.16-4.pdf, Stand: 07.02.2009.

Pousttchi (2003): Pousttchi, Key: Abrechnung mobiler Mehrwertdienste, in: Dittrich, K.; König, W.; Oberweis, A.; Rannenberg, K.; Wahlster, W. (Hrsg.): Informatik 2003 – Innovative Informatikanwendungen, Band 2, 2003, S. 408-413.

http://wi2.wiwi.uni-augsburg.de/pics/mobile/Uni-Augsburg_WI2-MC_MP-13-09.pdf, Stand: 07.02.2009.

Pousttchi (2005): Pousttchi, Key: Mobile Payment in Deutschland: Szenarienübergreifendes Referenzmodell für mobile Bezahlvorgänge, Diss., veröffentlicht von DUV, Gabler Verlag, Wiesbaden, 1. Aufl., 2005.

Rabbe/Jahnke (2001): Rabbe, Georg; Jahnke, Jennifer (Hrsg.): Praxishandbuch Call Center, 1. Auflage, Ecmc Gernot Gehrke-Verlag, Marl, 2001.

Ramzan/Ruhl (2000): Ramzan, Zulfikar; Ruhl, Matthias: Anonymous Subscription Protocols, MIT Laboratory for Computer Science, 545 Technology Square, Cambridge, MA 02139, USA, 2000.

http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.35.7149, Stand: 04.07.2009.

Reder (2009): Reder, Bernd: Gartner: Die zehn wichtigsten Mobilanwendungen im Jahr 2012, in: Networkcomputing.de, Trends & Märkte. Online-Artikel, publiziert am 23.11.2009.

http://www.networkcomputing.de/trends-maerkte/artikel-8530.html, Stand: 09.01.2010.

Reichenbach (2002): Reichenbach, Martin: Elektronische Zahlungssysteme – Eine einführende Darstellung, in: Sauerburger, H.: Zahlungssysteme - E-Banking, in: HMD 224, Praxis der Wirtschaftsinformatik, dpunkt.verlag, Heidelberg, 2002, S.7-21.

Reiter/Rubin (1997): Reiter, Michael K.; Rubin, Aviel D.: Crowds: Anonymity for Web Transactions. AT&T Labs-Research, DIMACS Technical Report 97-15, April 1997.

http://www.cise.ufl.edu/~pharsh/public/cis6930/crowds-anonymity-for-web.pdf, Stand: 30.10.2009.

Robben (2001): Robben, Matthias: Location Based Services - Standortvorteile nutzen, in: ECIN, Online-Artikel, publiziert am 29.03.2001.

http://www.ecin.de/mobilebusinesscenter/lbs/index.html, Stand: 23.02.2010.

Ronzheimer (2005): Ronzheimer, Manfred: Das Handy ist zum Parken da!, in: TelematicsMONITOR, Nr. 1, Juni 2005, Berlin, 2005, S. 4-6.

http://telematicspro.de/telematicspro/Downloads/TM_01_0605.pdf, Stand: 21.02.2010.

Rost (2003): Rost, Martin: Zur gesellschaftlichen Funktion von Anonymität - Anonymität im soziologischen Kontext, in: Datenschutz und Datensicherheit (DuD), Nr. 27/3, Seiten 156-158, 2003.

http://www.maroki.de/pub/privacy/dud3anon.pdf, Stand: 28.10.2009.

Ruedin (2009): Ruedin, Etienne: Identitäten im Internet – das Ende der Anonymität? Verlag Benziger-Emosson, Zürich, 2009.

http://www.lulu.com/items/volume_64/6310000/6310957/1/print/EBUS-Buch.pdf, Stand: 24.10.2009.

Sam (2009): Sam, Kristina: Mobiles Banking Chance für Entwicklungsländer, in: pressetext.com, Online-Artikel, publiziert am 23.02.2009.

http://pressetext.com/news/090223001/, Stand: 15.02.2010.

Sauerburger (2002): Sauerburger, Heinz: Zahlungssysteme - E-Banking, in: HMD 224, Praxis der Wirtschaftsinformatik, dpunkt.verlag, Heidelberg, 2002.

Scheible (2007): Scheible, Joachim: Pay-Buy-Mobile Initiative startet, in: Connect.de, Online-Artikel, publiziert am 14.11.2007.

http://www.connect.de/news/Pay-Buy-Mobile-Initiative-startet_387675.html, Stand: 22.02.2010.

Schemberg/Linten (2006): Schemberg, Axel; Linten, Martin: PC-Netzwerke, 3. Ausgabe, Galileo Press, Bonn, 2006.

Schöning (2006): Schöning, Uwe: Ideen der Informatik: Grundlegende Modelle und Konzepte, 2. Auflage, Oldenbourg Wissenschaftsverlag, München.

Schonschek (2009): Schonschek, Oliver: Twitter: Nicht nur harmloses Gezwitscher, in: Datenschutz-PRAXIS, Online-Artikel, publiziert am 20.04.2009.

http://www.datenschutz-praxis.de/fachwissen/fachartikel/twitter-nicht-nur-harmloses-gezwitscher/, Stand: 26.02.2010.

Schröder/Rödl (2004): Schröder, H.; Rödl, A.: Der Nutzen von Transaktionsdaten für das Handelsmarketing in: Trommsdorff. In: Handelsforschung, Köln 2004, S. 519-538.

http://www.marketing.wiwi.uni-due.de/uploads/tx_itochairt3/publications/2004_Transaktionsdaten.pdf, Stand: 11.08.2009.

Schuba (2004): Schuba, Marco: Payment Systems for Use in Mobile Networks, Präsentationsunterlagen, Ericsson Research, Aachen, 2004, S. 1-14.

http://www.ovum.com/mocca/content/tt2/pay.pdf, Stand: 27.09.2009.

Schütz (2006): Schütz, Joe: Security: Firewall und Proxy, Version: 4.0, Copyright: Educaid GmbH, 2006.

Schwark (2004): Schwark, Bastian: Anonymisierungsdienste im Internet, in: Karlsruher Transfer, Nr. 30, S. 26-31, Karlsruhe, 2004.

http://www.fuks.org/fileadmin/download/transfer/kt30/KT30_Seiten26-31-Anonymisierung.pdf, Stand: 04.01.2009.

Seiffert (2006): Seiffert, Hannah: Anonymisierungsdienste als Geschäftsmodelle für Provider? Präsentationsunterlagen, Abschlussveranstaltung des BMWi-Projektes „Starke Anonymität und Unbeobachtbarkeit im Internet“ 24.11.2006, BMWi, Berlin.

http://anon.inf.tu-dresden.de/bmwi2006/Seiffert2006-11-24BMWIANON.pdf, Stand: 05.02.2010.

Sekino/Kwon/Bong (2007): Sekino, Hamilton; Kwon, John; Bong, Se Han: Mobile Payments: Mobile Operator Market Opportunities and Business Models, PerpeDiamond Management & Technology Consultants, Chicago, 2007.

http://www.diamondconsultants.com/PublicSite/ideas/perspectives/downloads/INSIGHT%20-%20Mobile%20Payments%20_Diamond.pdf, Stand: 15.03.2009.

SEMOPS (2008): SEMOPS (Secure Mobile Payment Service) Brochure, SEMOPS H-1022 Budapest, Beg u. 3-5, Hungary, www.semops.com, 2008.

http://www.semops.com/uploadfiles/SEMOPS_Broschure_2008.pdf, Stand: 06.02.2010.

Silberer/Wohlfahrt/Wilhelm (2002): Silberer, Günter; Wohlfahrt, Jens; Wilhelm, Thorsten: Mobile Commerce – Grundlagen, Geschäftsmodelle, Erfolgsfaktoren, Gabler Verlag, Wiesbaden, 2002.

Scholz (2008): Scholz, Heike: Twitpay: Geld schicken mit Twitter, in: Mobile Zeitgeist, Online-Artikel, publiziert am 20.11.2008.

http://www.mobile-zeitgeist.com/2008/11/20/twitpay-geld-schicken-mit-twitter/, Stand: 28.01.2010.

Spann/Zuber (2003): Spann, Martin; Zuber, Markus: Der Trade-Off zwischen dem Wunsch nach Anonymität und Vertrauen im Internet: Hemmnis für den Electronic Commerce?, in: Jahrbuch der Absatz- und Verbrauchsforschung, Nr. 2, S. 185-205, 2003.

http://www.marketing.uni-passau.de/fileadmin/pubs/Spann_Zuber_GfK.pdf, Stand: 24.10.2009.

Stahlknecht/Hasenkamp (2005): Stahlknecht, Peter; Hasenkamp, Ulrich: Einführung in die Wirtschaftsinformatik. 11. Auflage, Springer-Verlag, Berlin, Heidelberg, New York, 2005.

Stadler (2006): Stadler, Tobias: Mobiles Bezahlen. Die rechtsverträgliche Gestaltung mobiler Bezahlverfahren in Deutschland, Nomos-Verlag, Baden-Baden, 2006.

Sternberger (2003): Sternberger, David: Security in Safety Critical Systems, Institut für Technische Informatik, Technische Universität Wien, Wien, 2003.

http://www.vmars.tuwien.ac.at/courses/akti12/journal/03ss/article_03ss_Sternberger.pdf, Stand: 28.02.2010.

Swoboda/Spitz/Pramateftakis (2008): Swoboda, Joachim; Spitz, Stephan; Pramateftakis, Michael: Kryptographie und IT-sicherheit: Grundlagen und Anwendungen-eine Einführung, Vieweg+Teubner-Verlag, Wiesbaden, 2008.

Szugat et al. (2006): Szugat, Martin; Gewehr, Jan Erik; Lochmann, Cordula: Social Software. schnell + kompakt. 1. Kapitel, Seiten 1-18. entwickler.press - ein Imprint der Software & Support Verlag, Frankfurt, 2006.

http://entwickler.de/mediapool/szugat_social_software_Kap1.pdf, Stand: 24.10.2009.

Tatli/Stegemann/Lucks (2006): Tatli, Emin I.; Stegemann, Dirk; Lucks, Stefan: Dynamic Mobile Anonymity with Mixing, Technical Report / Department for Mathematics and Computer Science, University of Mannheim, TR-2006-007, 2006. S. 1-11.

http://th.informatik.uni-mannheim.de/people/tatli/pub/mdawm.pdf, Stand: 28.10.2009.

Teichmann/Nonnenmacher/Henkel (2001): Teichmann, Rene; Nonnenmacher, Martin; Henkel, Joachim: E-Commerce und E-Payment: Rahmenbedingungen, Infrastruktur, Perspektiven. Gabler Verlag, Wiesbaden, 2001.

Trappe (2007): Trappe, Yvonne: Die wirtschaftliche Bedeutung mobiler Datendienste im Mobilfunkmarkt, Akademische Schriftenreihe, GRIN-Verlag, Norderstedt, 2007.

Turowski/Pousttchi (2004): Turowski, Klaus; Pousttchi, Key: Mobile Commerce: Grundlagen und Techniken, Springer-Verlag, Berlin [u. a.], 2004.

ULD (2002): Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (Hrsg.), Broschüre: Sicherheit im Internet durch Anonymität, 2002.

https://www.datenschutzzentrum.de/download/anonheft.pdf, Stand: 27.01.2010.

Van Bruwaene (2006): Van Bruwaene, Kris: An Introduction in to Revenue Sharing, in: EBU TECHNICAL REVIEW - April 2006, Grand-Saconnex-Geneva, Switzerland, 2006.

http://www.ebu.ch/en/technical/trev/trev_306-van_bruwaene.pdf, Stand: 20.02.2010.

Vatter (2010): Vatter, André: Flattr: Pirate Bay-Gründer Peter Sunde will Paid Content revolutionieren, in: Basic Thinking Blog, Online-Artikel, publiziert am 11.02.2010.

http://www.basicthinking.de/blog/2010/02/11/flattr-pirate-bay-gruender-peter-sunde-will-paid-content-revolutionieren/, Stand: 26.02.2010.

Weigert (2010): Weigert, Martin: Flattr: Neuer Micropaymentdienst setzt auf die "Thank You Economy", in: Netzwertig.com, Online-Artikel, publiziert am 11.02.2010.

http://netzwertig.com/2010/02/11/flattr-neuer-micropaymentdienst-setzt-auf-die-thank-you-economy/, Stand: 26.02.2010.

Wikipedia (2010a): Anonymität, http://de.wikipedia.org/wiki/Anonymität, Stand: 12. 03.2010.

http://de.wikipedia.org/w/index.php?title=Spezial:Buch&bookcmd=download&collection_id=5795f4c5bbd0d188&writer=rl&return_to=Anonymit%C3%A4t, Stand: 12.03. 2010.

Wikipedia (2010b): Anonymity, http://en.wikipedia.org/wiki/Anonymity, Stand: 12.03. 2010.

http://en.wikipedia.org/w/index.php?title=Anonymity&printable=yes, Stand: 12.03.20 10.

Wilde/Hess (2006): Wilde, Thomas; Hess, Thomas: Methodenspektrum der Wirtschaftsinformatik: Überblick und Portfoliobildung, Arbeitsbericht Nr. 2/2006, Hrsg.: Prof. Dr. Thomas Hess, München.

http://www.wim.bwl.uni-muenchen.de/download_free/sonstiges/ab_2006_02.pdf, Stand: 15.01.2009.

Wishart (2006): Wishart, Neville: Micro-Payment Systems and Their Application to Mobile Networks. Washington, DC: infoDev / World Bank.

http://www.infodev.org/en/Publication.43.html, Stand: 01.03.2009.

Wislsperger (1998): Wislsperger, Robert: Trust-Center bilden die Basis für einen sicheren E-Commerce, in: Computerwoche.de, Online-Artikel, publiziert am 10.07. 1998.

http://www.computerwoche.de/heftarchiv/1998/28/1092485/, Stand: 25.02.2010.

Wohlmacher (2000): Wohlmacher, Petra: Sicherheitsanforderungen und Sicherheitsmechanismen bei IT-Systemen, Universität Klagenfurt, Institute für Informatik – Systemsicherheit, Klagenfurt, 2000.

http://subs.emis.de/LNI/EMISA-Forum/Volume20_1/wohlmacher.pdf, Stand: 28.02. 2010.

WPR 2008 (2008): World Payment Report 2008, Capgemini, RBS and EFMA, 2008.

http://www.keieiken.co.jp/services/financial/WPR08/pdf/WPR2008_English.pdf, Stand: 12.01.2010.

Zerfos et al. (2006): Zerfos, Petros; Meng, Xiaoqiao; Wong, Starsky H. Y.; Samanta, Vidyut; Lu, Songwu: A study of the short message service of a nationwide cellular network. Internet Measurement Conference 2006, October 25–27, 2006, Rio de Janeiro, Brazil, 2006, S. 263-268.

http://www.cs.ucla.edu/wing/publication/papers/Zerfos.IMC06.pdf, Stand: 28.01.2010.

Zischke (2008): Zischke, Joachim: Modelle unserer Identität, in: DIALOGUS Magazin, Online-Artikel, publiziert am 02. Oktober 2008.

http://www.dialogus.de/magazin/ideen/99, Stand: 24.10.2009.

Zhou/Bergmann/Schlang (2004): Zhou, Yi; Bergmann, Rasmus; Schlang, Harald: Geschäftsmodelle für Mobile Financial Services, in: Mellis, W.; Trittmann, R. (Hrsg.): Studien zur Systementwicklung, Band 18, Lehrstuhl für Wirtschaftsinformatik-Systementwicklung, Universität zu Köln, 2004.

http://systementwicklung-archiv.bibliothek.informatik.uni-koeln.de/30/1/Band18_2004.pdf, Stand: 24.02.2010.

Feyyat Kaymaz

Der Schutz der persönlichen Daten vor Manipulation und Missbrauch gewinnt in mobilen Kommunikationsnetzwerken zunehmend an Bedeutung. Immer mehr Menschen fragen sich, was mit im Mobile Commerce hinterlassenen Daten und Informationen geschieht, wenn sie Mobile Payments nutzen. Diese Daten und Informationen verschaffen Potenziale für die Erstellung individueller und kollektiver Persönlichkeitsprofile, Betrug, Manipulation und Missbrauch. Es fehlt die User-Anonymität in den vorhandenen Mobile Payment Systemen. Die User-Anonymität stellt somit eine wichtige Anforderung dar und bietet einen enormen Kundennutzen für die Akzeptanz und Nutzung von Mobile Payment.

In dieser Dissertation sollten neue Paradigmen, die zur Lösung der Problematik beitragen, entwickelt beziehungsweise angewendet werden. Hierfür wurden die Rahmenbedingungen sowie die vorhandenen und neuen potentiellen Gestaltungsmöglichkeiten zur Herstellung und Bewahrung der User-Anonymität untersucht. Das vorgeschlagene Referenzprozessmodell wurde mittels Heranziehung der existierenden Anonymitätskonzepte entwickelt und ermöglicht es mobilen Usern, anonyme Mobile Payments zu nutzen. Der mobile User ist damit in der Lage, selber zu entscheiden, ob und wann er anonym bleiben möchte.

ISBN 978-3-86219-192-5