

Stephanie Kretschmar

**Elektronische Zahlungssysteme -
Verbreitung und Akzeptanz im B2C Bereich**

Diplomarbeit

BEI GRIN MACHT SICH IHR WISSEN BEZAHLT



- Wir veröffentlichen Ihre Hausarbeit, Bachelor- und Masterarbeit
- Ihr eigenes eBook und Buch - weltweit in allen wichtigen Shops
- Verdienen Sie an jedem Verkauf

Jetzt bei www.GRIN.com hochladen
und kostenlos publizieren



**Fachhochschule für Ökonomie und Management
Essen**

**Diplomarbeit
zur
Diplom-Informatikerin**

**Thema
Elektronische Zahlungssysteme
Verbreitung und Akzeptanz im B2C Bereich**

vorgelegt von: Stephanie Kretschmar

Marl, den 28.02.2005

Inhaltsverzeichnis

| | |
|---|-------------|
| Inhaltsverzeichnis | III |
| Abbildungsverzeichnis..... | VII |
| Glossar | VIII |
| 1 Einleitung | 1 |
| 2 Technologie der Zahlungssysteme | 2 |
| 2.1 Verschlüsselungsverfahren..... | 2 |
| 2.1.1 Symmetrische Verschlüsselungsverfahren | 3 |
| 2.1.2 Asymmetrische Verschlüsselungsverfahren | 4 |
| 2.1.3 Hybride Verschlüsselungsverfahren | 5 |
| 2.1.4 RSA | 6 |
| 2.1.4.1 RSA- Algorithmus | 6 |
| 2.1.4.2 RSA- Verschlüsselung..... | 7 |
| 2.1.4.3 RSA- Entschlüsselung | 8 |
| 2.1.5 Public Key Infrastructure - PKI | 9 |
| 2.1.5.1 Zertifizierungsstellen | 10 |
| 2.1.5.2 Kerberos | 11 |
| 2.2 Authentifizierungsverfahren..... | 12 |
| 2.2.1 Digitale Signaturen | 13 |
| 2.2.2 Challenge Response | 14 |
| 2.2.3 Persönliche Identifikationsnummer - PIN..... | 15 |
| 2.3 Elektronische Zahlungssysteme mit Terminals..... | 15 |
| 2.3.1 Electronic Cash | 16 |
| 2.3.2 Point of Sale ohne Zahlungsgarantie - POZ..... | 17 |
| 2.3.3 Elektronisches Lastschriftverfahren..... | 18 |
| 2.3.4 Geldkarte..... | 20 |
| 2.3.4.1 Zahlungen im Handel..... | 21 |
| 2.3.4.2 Zahlungen im Internet..... | 21 |
| 2.3.4.3 Verbreitung | 22 |
| 2.3.4.4 Kosten | 23 |
| 2.3.5 Kreditkarte | 23 |
| 2.3.5.1 Technische Voraussetzungen..... | 24 |
| 2.3.5.2 Kosten | 24 |
| 2.3.5.3 Authentifizierung | 25 |
| 2.4 Elektronische Zahlungssysteme im Internet..... | 26 |
| 2.4.1 Kreditkarte | 26 |
| 2.4.1.1 Secure Socket Layer - SSL | 27 |
| 2.4.1.1.1 Technische Voraussetzungen und Kosten | 27 |
| 2.4.1.1.2 Kommunikation | 28 |
| 2.4.1.1.3 Authentifizierung..... | 28 |

| | | |
|-----------|---|-----------|
| 2.4.1.2 | Secure Electronic Transaction - SET | 29 |
| 2.4.1.2.1 | Technische Voraussetzungen und Registrierung | 30 |
| 2.4.1.2.2 | Kommunikation | 32 |
| 2.4.1.2.3 | Authentifizierung | 34 |
| 2.4.2 | Lastschriftverfahren | 34 |
| 2.4.2.1 | Virtuelle Terminals | 35 |
| 2.4.2.2 | Automatisierte Anwendungen | 36 |
| 3 | Rechtlicher Rahmen | 37 |
| 3.1 | Elektronische Signatur | 37 |
| 3.1.1 | Herkömmliche elektronische Signatur | 38 |
| 3.1.2 | Fortgeschrittene elektronische Signatur | 38 |
| 3.1.3 | Qualifizierte elektronische Signatur | 38 |
| 3.1.4 | Beweiskraft von elektronischen Signaturen | 39 |
| 3.2 | Datenschutz | 39 |
| 3.2.1 | Grenzüberschreitender Datenaustausch | 40 |
| 3.2.2 | Bundesdatenschutzgesetz - BDSG | 40 |
| 3.2.2.1 | Begriffserklärungen | 41 |
| 3.2.2.1.1 | Personenbezogene Daten - § 3 Abs. 1 BDSG | 41 |
| 3.2.2.1.2 | Dateien - § 3 Abs. 2 BDSG | 41 |
| 3.2.2.1.3 | Datenerhebung - § 3 Abs. 4 BDSG | 41 |
| 3.2.2.1.4 | Speichern, Verändern, Übermitteln, Löschen, Sperrern und Nutzen von Daten - § 3 Abs. 5 & 6 BDSG | 42 |
| 3.2.2.1.5 | Anonymisieren und Pseudonymisieren - § 3 Abs. 7 BDSG | 42 |
| 3.2.2.1.6 | Verantwortliche Stelle, Empfänger, Dritte - § 3 Abs. 8 & 9 BDSG | 42 |
| 3.2.2.2 | Wichtige Paragraphen für elektronische Zahlungssysteme | 43 |
| 3.2.2.2.1 | Vorschriften für mobile Speicher- und Verarbeitungsmedien | 43 |
| 3.2.2.2.2 | Automatische Verarbeitung personenbezogener Daten | 44 |
| 3.2.2.2.3 | Verantwortliche für die Einhaltung des Datenschutzes | 44 |
| 3.3 | Elektronische Zahlungssysteme | 44 |
| 3.3.1 | Rechtsgrundlagen für Kreditkarten | 45 |
| 3.3.2 | Rechtsgrundlagen für Lastschriftverfahren | 45 |
| 3.3.3 | Rechtsgrundlagen für die Geldkarte | 46 |
| 4 | Wirtschaftliche Bedeutung | 47 |
| 4.1 | Unternehmen | 47 |
| 4.1.1 | Rationalisierung | 48 |
| 4.1.2 | Umsatzsteigerung | 48 |
| 4.1.3 | Kosteneinsparungen | 49 |
| 4.1.3.1 | Transaktionskosten | 49 |

| | | |
|----------|--|-----------|
| 4.1.3.2 | Kostenreduzierung durch Virtuelle Terminals..... | 50 |
| 4.1.3.3 | Kosteneinsparungen durch automatisierte Prozesse | 50 |
| 4.1.4 | Sicherheit | 51 |
| 4.1.4.1 | Magnetstreifenkarten | 52 |
| 4.1.4.2 | Persönliche Identifikationsnummer - PIN | 53 |
| 4.1.4.3 | Geldkarte | 53 |
| 4.1.5 | Verlässlichkeit..... | 54 |
| 4.1.6 | Steigerung der Serviceleistungen..... | 54 |
| 4.2 | Kunden | 55 |
| 4.2.1 | Flexibilität | 55 |
| 4.2.2 | Verfügbarkeit | 55 |
| 4.2.3 | Anonymität..... | 56 |
| 5 | Akzeptanz und Affinität | 57 |
| 5.1 | Anforderungen an elektronische Zahlungssysteme..... | 58 |
| 5.1.1 | Verbreitung und Marktdurchdringung..... | 59 |
| 5.1.2 | Sicherheit | 59 |
| 5.1.3 | Zahlungszeitpunkt..... | 59 |
| 5.1.4 | Zahlungsbereich | 60 |
| 5.1.5 | Kosten | 60 |
| 5.1.6 | Anonymität..... | 60 |
| 5.1.7 | Bedienbarkeit | 60 |
| 5.1.8 | Geschwindigkeit..... | 61 |
| 5.1.9 | Skalierbarkeit | 61 |
| 5.1.10 | Stornierungsmöglichkeiten | 61 |
| 5.1.11 | Absicherung im Schadensfall..... | 61 |
| 5.2 | Bewertung elektronischer Zahlungssysteme | 62 |
| 5.2.1 | Kreditkartenzahlung..... | 62 |
| 5.2.1.1 | Verbreitung und Marktdurchdringung..... | 62 |
| 5.2.1.2 | Sicherheit | 63 |
| 5.2.1.3 | Zahlungszeitpunkt..... | 64 |
| 5.2.1.4 | Zahlungsbereich..... | 64 |
| 5.2.1.5 | Kosten | 64 |
| 5.2.1.6 | Anonymität | 65 |
| 5.2.1.7 | Bedienbarkeit & Geschwindigkeit..... | 65 |
| 5.2.1.8 | Skalierbarkeit | 65 |
| 5.2.1.9 | Stornierungsmöglichkeiten | 65 |
| 5.2.1.10 | Absicherung im Schadensfall | 66 |
| 5.2.1.11 | Zusammenfassung..... | 66 |
| 5.2.2 | Lastschriftverfahren | 67 |
| 5.2.2.1 | Verbreitung und Marktdurchdringung..... | 67 |
| 5.2.2.2 | Sicherheit | 68 |
| 5.2.2.3 | Zahlungszeitpunkt..... | 68 |
| 5.2.2.4 | Zahlungsbereich..... | 69 |

| | | |
|----------|--|-----------|
| 5.2.2.5 | Kosten | 69 |
| 5.2.2.6 | Anonymität | 69 |
| 5.2.2.7 | Bedienbarkeit & Geschwindigkeit..... | 69 |
| 5.2.2.8 | Skalierbarkeit | 70 |
| 5.2.2.9 | Stornierungsmöglichkeiten | 70 |
| 5.2.2.10 | Absicherung im Schadensfall | 70 |
| 5.2.2.11 | Zusammenfassung..... | 70 |
| 5.2.3 | Geldkarte..... | 71 |
| 5.2.3.1 | Verbreitung und Marktdurchdringung..... | 71 |
| 5.2.3.2 | Sicherheit | 71 |
| 5.2.3.3 | Zahlungszeitpunkt..... | 72 |
| 5.2.3.4 | Zahlungsbereich..... | 72 |
| 5.2.3.5 | Kosten | 72 |
| 5.2.3.6 | Anonymität | 73 |
| 5.2.3.7 | Bedienbarkeit & Geschwindigkeit..... | 73 |
| 5.2.3.8 | Skalierbarkeit | 73 |
| 5.2.3.9 | Stornierungsmöglichkeiten | 73 |
| 5.2.3.10 | Absicherung im Schadensfall | 73 |
| 5.2.3.11 | Zusammenfassung..... | 74 |
| 5.2.4 | Vergleich elektronischer Zahlungssysteme | 74 |
| 5.3 | Umfrageergebnis | 76 |
| 5.3.1 | Aufbau der Umfrage | 76 |
| 5.3.2 | Ergebnisse der Umfrage..... | 77 |
| 5.3.3 | Zusammenfassung..... | 83 |
| 6 | Fazit | 84 |
| | Literaturverzeichnis | 86 |

Abbildungsverzeichnis

| | |
|---|----|
| Abbildung 1: Symmetrische Verschlüsselung..... | 3 |
| Abbildung 2: Asymmetrische Verschlüsselung | 4 |
| Abbildung 3: Hybride Verschlüsselungsverfahren | 5 |
| Abbildung 4: Public Key Infrastructure mit Zertifizierungsstellen | 10 |
| Abbildung 5: Public Key Infrastructure mit Kerberos Server | 11 |
| Abbildung 6: Digitale Signatur | 13 |
| Abbildung 7: Challenge Response | 14 |
| Abbildung 8: Electronic Cash, altes Logo..... | 16 |
| Abbildung 9: Electronic Cash, neues Logo | 16 |
| Abbildung 10: MASTERCARD Logo | 17 |
| Abbildung 11: Point of Sale ohne Zahlungsgarantie Logo..... | 18 |
| Abbildung 12: Elektronisches Lastschriftverfahren Logo | 19 |
| Abbildung 13: Geldkarte Logo..... | 20 |
| Abbildung 14: Geldkartenzahlung im Internet..... | 22 |
| Abbildung 15: VISA Logo | 23 |
| Abbildung 16: MASTERCARD Logo | 23 |
| Abbildung 17: VISA/ MASTERCARD Classic | 24 |
| Abbildung 18: VISA/ MASTERCARD Gold..... | 24 |
| Abbildung 19: SET - Kundenregistrierung | 30 |
| Abbildung 20: SET - Händlerregistrierung | 32 |
| Abbildung 21: SET - Bestellabwicklung..... | 33 |
| Abbildung 22: Aufteilung der Befragten nach Geschlecht und Alter | 77 |
| Abbildung 23: Bekanntheitsgrad und Nutzung im Handel..... | 78 |
| Abbildung 24: Bekanntheitsgrad und Internetnutzung | 79 |
| Abbildung 25: Vorteile elektronischer Zahlungssysteme | 82 |
| Abbildung 26: Nachteile elektronischer Zahlungssysteme..... | 83 |

Glossar

| | |
|--------------------------------------|--|
| Acquirer | Vertragsunternehmen eines Händlers, welches die Kartendaten autorisiert, erfasst und Zahlungen transferiert. |
| Authentifizierung | Verfahren zur Überprüfung der Identität, dies kann mit Hilfe von Passwörtern, Chipkarten oder biometrischen Verfahren realisiert werden. |
| Asymmetrische Verschlüsselung | Verschlüsselungsverfahren, bei dem zwei Schlüssel verwendet werden; ein Schlüssel zum Verschlüsseln und einer zum Entschlüsseln. |
| B2C | Kurzform von Business-to-Consumer, bezeichnet Geschäftsbeziehungen zwischen Händlern und Privatkunden. |
| Challenge Response | Verfahren, bei dem die Autorisierung über persönliches Geheimnis erfolgt; wird unter anderem bei EC-Karten mit PIN eingesetzt. |
| Digitale Signatur | Daten, die elektronischen Nachrichten hinzugefügt werden und der Authentifizierung dienen. |
| Disagio | Gebühr, die ein Händler für Kartentransaktionen an Acquirer oder entsprechendes Vertragsunternehmen zahlt. |
| Hash- Funktion | Verfahren, welches zur Komprimierung von Nachrichten und Daten dient. Aus einer Nachricht wird ein Wert mit fester Länge berechnet, der so genannte Hash- Wert. Dieser ist der Nachricht eindeutig zuzuordnen, da eine Veränderung in der Nachricht zu einem veränderten Hash- Wert führt. Rückschlüsse vom Hash- Wert auf die Nachricht sind nicht möglich. |

| | |
|--|--|
| Hybride Verschlüsselung | Kombination aus symmetrischer und asymmetrischer Verschlüsselung. Eine Nachricht wird symmetrisch verschlüsselt. Der verwendete Schlüssel wird mit dem öffentlichen Schlüssel des Empfängers verschlüsselt, so dass nur der Empfänger (Inhaber des privaten Schlüssels) den Schlüssel und anschließend die Nachricht entschlüsseln kann. |
| Kerberos | Dienst der auf einem Server aktiviert ist und die Authentifizierung durch die Verteilung und Verwaltung von Sitzungsschlüsseln regelt. |
| Persönliche Identifikationsnummer (PIN) | Persönliches Geheimnis, welches aus Zahlen- und/ oder Buchstabenkombinationen besteht und der Authentifizierung dient. |
| Public Key Infrastructure (PKI) | Methode für die Erstellung, Ausgabe und Verwaltung von Zertifikaten und digitalen Signaturen. |
| Random Access Memory (RAM) | Speicher, der lesbar, adressierbar und beschreibbar ist; speichert die Daten nur solange eine Stromversorgung vorhanden ist. |
| Read Only Memory (ROM) | Speicher, der lesbar, aber nicht wieder beschreibbar ist. |
| RSA | Asymmetrisches Verschlüsselungsverfahren, 1978 veröffentlicht und nach seinen Erfindern Ron Rivest, Adi Shamir und Leonard Adleman benannt. |
| Secure Electronic Transaction (SET) | Protokoll zur sicheren Datenübertragung im Internet, speziell für sensible Daten entwickelt. Verwendet Zertifikate bei allen Vertragspartnern und garantiert die eindeutige Identifizierung. |