Inhalt

1 **Einführung** ... 1

2 **Eigenschaften elektronischer Zahlungssysteme** ... 7
2.1 Systemsicherheit elektronischer Zahlungssysteme ... 8
2.1.1 Datenübertragung ... 8
2.1.2 Authentifizierung und Identitätsnachweis ... 10
2.1.3 Mechanismen zum Schutz der Hardware ... 15
2.2 Transaktionskosten ... 16
2.2.1 Hohe Transaktionskosten ... 16
2.2.2 Mittlere Transaktionskosten ... 17
2.2.3 Niedrige Transaktionskosten ... 17
2.3 Rückverfolgbarkeit von Zahlungen ... 18
2.3.1 Uneingeschränkte Rückverfolgbarkeit ... 20
2.3.2 Eingeschränkte Rückverfolgbarkeit (Verknüpfbarkeit von Zahlungen) ... 20
2.3.3 Nicht rückverfolgbare Zahlungen ... 21
2.3.4 Benutzergesteuerte Rückverfolgbarkeit ... 21
2.4 Online-Überprüfungserfordernisse ... 22
2.5 Akzeptanzfähigkeit ... 23
2.6 Übertragbarkeit ... 23
2.7 Teilbarkeit ... 24
2.8 Reine Software-Lösungen kontra fälschungssichere Hardware ... 25
2.9 Schlußbetrachtung ... 25

3 **Basiskonzepte für elektronische Finanztransaktionssysteme** ... 29
3.1 Das Überweisungssystem ... 30
3.2 Das Schecksystem ... 31
3.3 Das Einweg-Token-System ... 32
3.4 Das Mehrweg-Token-System ... 36
3.5 Das System des sicheren Zählers ... 37
3.6 Schlußfolgerung ... 38

4 Zahlungsprotokolle für das Internet 41
4.1 iKP – Internet Keyed Payment Protocols
Verschlüsselte Abwicklungsprotokolle
für Zahlungen im Internet 41
4.2 STT – Secure Transaction Technology
Technologie zur sicheren Durchführung von Transaktionen 43
4.3 SEPP – Secure Electronic Payment Protocol
Sicheres elektronisches Zahlungsprotokoll 46
4.4 SEPP kontra STT. 51
4.5 SET – der Nachfolger von STT und SEPP 52
4.6 Elektronisches Bargeld von Chaum 54
4.7 Millicent 58

5 Implementierte Internetsysteme 63
5.1 ecash (von DigiCash) 63
5.2 First Virtual 66
5.3 CyberCash 68
5.4 NetCash 71
5.5 CheckFree 73
5.6 CARI 74

**6 Smart-Card-Geld –
Geld auf intelligenten Chipkarten** 77
6.1 Das Basisdesign eines chipkartenbasierten
Wertkartensystems (SVC-System) 79
6.2 Ein einfaches Protokoll
für ein Wertkartensystem mit geheimem Schlüssel 80
6.2.1 Personalisierung der Karten 81
6.2.2 Transaktion des Wiederaufladens 81
6.2.3 Belastungstransaktion 82
6.2.4 Übertragung (Download) der Terminal-Transaktionen 82
6.3 Offene kontra geschlossene Systeme 82
6.4 Chipkarten und Datenschutz 85
6.5 Bestehende Systeme und Systeme im Versuchsstadium 86
6.5.1 Danmønt 87
6.5.2 Proton 88
6.5.3 MasterCard Cash 89
6.5.4 Mondex 90
6.5.5 CAFE 92

7 Die Folgen neuer Zahlungssysteme ... 93
7.1 Folgen für das Geldsystem ... 94
7.1.1 Sinkende Bargeldnachfrage ... 94
7.1.2 Verlust von Seignorage ... 96
7.1.3 Free Banking und Zentralbankkontrolle des Computergeldes ... 96
7.1.4 Anstieg der Umlaufsgeschwindigkeit ... 98
7.2 Politische und gesetzestechnische Fragen elektronischer Zahlungen ... 98
7.2.1 Die Datenschutzdebatte ... 99
7.2.2 Elektronische Geldwäsche ... 103
7.2.3 Steuerflucht ... 105
7.2.4 Zertifizierungscenter ... 107

8 Anhang: Kryptographische Techniken ... 111
8.1 Kryptosysteme mit asymmetrischem Schlüsselpaar (Public Key Cryptosystems) ... 111
8.2 Unumkehrbare Hashfunktionen und message digest (Nachrichten-Prüfsumme) ... 114
8.3 Elektronische Signaturen ... 115
8.4 Elektronische Beglaubigungen und Zertifikate ... 117
8.5 Blinde Signaturen ... 119

Literaturverzeichnis ... 121

Index ... 125