

Inhalt

1 Einführung	1
1.1 Historische Entwicklung	1
1.1.1 Historische Entwicklung von RFID	1
1.1.2 Historische Entwicklung der Chipkarten	2
1.1.3 Historische Entwicklung von NFC	4
1.1.4 Die NFC-Technologie	6
1.2 Das NFC Forum	7
1.3 Die ersten Mikrochips, Geräte und Hersteller	9
1.3.1 NFC-ICs	9
1.3.2 Mobiltelefone	9
Literatur	11
2 Technische Grundlagen	13
2.1 Induktive Kopplung	13
2.1.1 Magnetisches Feld	14
2.1.2 Magnetische Spannung	14
2.1.3 Magnetische Feldstärke	14
2.1.4 Magnetische Flussdichte	16
2.1.5 Magnetischer Fluss	16
2.1.6 Induktivität	16
2.1.7 Gegeninduktivität	17
2.1.8 Kopplungsfaktor	18
2.1.9 Induktion	18
2.1.10 Transformator	19
2.1.11 Schwingkreis	20
2.2 Energieversorgung	21
2.3 Datenübertragung	22
2.3.1 Modulationsverfahren	23
2.3.2 Codierungsverfahren	24
2.3.3 Datenübertragung vom Lesegerät zum Transponder	25
2.3.4 Datenübertragung vom Transponder zum Lesegerät	26

2.4 Mehrfachzugriffsverfahren	27
2.4.1 Antikollision	28
Literatur	32
3 Smartcard Technologie	33
3.1 Definition: Smartcard	33
3.2 Klassifizierung	33
3.2.1 Funktionalität	34
3.2.2 Kommunikationsschnittstelle	36
3.3 Physikalische Eigenschaften	39
3.3.1 Identifikationskarten nach ISO/IEC 7810	40
3.3.2 Kontaktbehaftete Chipkarten nach ISO/IEC 7816	41
3.3.3 Kontaktlose Chipkarten nach ISO/IEC 14443	42
3.4 Übertragungsprotokolle	43
3.4.1 Kontaktbehaftete Chipkarten nach ISO/IEC 7816	45
3.4.2 Kontaktlose Chipkarten nach ISO/IEC 14443	52
3.4.3 Vergleich der Standards ISO/IEC 7816 und ISO/IEC 14443 ...	55
3.4.4 FeliCa	56
3.4.5 ISO/IEC 15693	59
3.5 Aufbau von Smartcards	59
3.5.1 Speicherkarten	59
3.5.2 Prozessorkarten	60
3.5.3 Betriebssysteme	60
3.5.4 Dateisystem	65
3.5.5 Befehle	66
3.6 Sicherheit von Smartcard-Mikrochips	68
3.6.1 Klassifizierung von Angriffen	68
3.6.2 Attacken und Schutzmaßnahmen	69
Literatur	72
4 Beispiele für kontaktlose Chipkarten	75
4.1 MIFARE	75
4.1.1 MIFARE Ultralight	76
4.1.2 MIFARE Classic	77
4.1.3 MIFARE Application Directory	79
4.2 FeliCa	81
4.2.1 Dateisystem	81
4.2.2 Befehlssatz	82
Literatur	85
5 NFC-Technologie	87
5.1 Einführung und Überblick	87
5.1.1 Normierungsaktivitäten	87
5.1.2 Das NFC Forum	88
5.1.3 Zusammenspiel der Standards und Protokolle	89

5.2	Peer-to-Peer-Modus	91
5.2.1	Passiver Kommunikationsmodus	92
5.2.2	Aktiver Kommunikationsmodus	93
5.2.3	Initialisierung und Datenaustausch	95
5.2.4	Logical Link Control Protocol (LLCP)	97
5.3	Reader/Writer-Modus	99
5.4	Card-Emulation-Modus	100
5.5	Arbeitsweise	101
5.5.1	NFCIP-2	101
5.5.2	Mode Switching	102
5.5.3	Activities Spezifikation	104
5.6	Sicherheit	105
5.6.1	Angriffsmöglichkeiten	105
5.6.2	NFCIP-1 Security Services and Protocol (NFC-SEC)	106
	Literatur	107
6	Datenformate	109
6.1	NFC-Forum-Tags	109
6.1.1	Type 1	110
6.1.2	Type 2	114
6.1.3	Type 3	116
6.1.4	Type 4	117
6.2	NFC Data Exchange Format (NDEF)	120
6.2.1	NDEF Record	120
6.2.2	NDEF Message	122
6.3	MIME Media Types	123
6.4	NFC Record Type Definition (RTD)	123
6.4.1	NFC Forum Well-known Types	124
6.4.2	NFC Forum External Types	125
6.4.3	Text Record Type	125
6.4.4	URI Record Type	126
6.4.5	Smart Poster Record Type	127
6.4.6	Generic Control Record Type	130
6.4.7	Signature Record Type	133
6.4.8	Connection Handover	137
	Literatur	143
7	Architektur mobiler NFC-Geräte	145
7.1	NFC im Mobiltelefon: Zusammenspiel der Standards	145
7.1.1	Aufbau eines mobilen NFC-Geräts	146
7.1.2	Beteiligte Organisationen	146
7.2	NFC-Controller	153
7.2.1	Energieversorgung	153
7.3	Secure Element	155
7.3.1	Aufgaben und Anforderungen	155

7.3.2	Varianten.....	156
7.3.3	Aufbau und Funktionsweise	158
7.3.4	Lebenszyklus	160
7.3.5	Parallele Verwendung mehrerer Secure Elements.....	160
7.4	Host-/Basisbandcontroller	164
7.5	Schnittstellen von Secure Element und NFC-Controller.....	164
7.5.1	NFC Wired Interface (NFC-WI)	165
7.5.2	Single Wire Protocol (SWP).....	166
7.5.3	Host Controller Interface (HCI)	170
7.5.4	NFC Controller Interface (NCI)	173
7.6	Softwareentwicklung für mobile NFC-Geräte.....	173
7.6.1	Java Micro Edition (Java ME).....	174
7.6.2	Smartcard Webserver.....	182
7.6.3	Windows Mobile und andere Betriebssysteme.....	182
7.7	Sicherheitsaspekte	183
7.7.1	Schaltbare NFC-Funktion.....	183
7.7.2	Verbindung zwischen Secure Element und Hostcontroller	184
7.7.3	Sichere Ein- und Ausgabe	184
	Literatur.....	185
8	Over-the-Air (OTA) Management.....	187
8.1	Einleitung	187
8.2	GlobalPlatform.....	188
8.3	Trusted Service Manager.....	188
8.4	GlobalPlatform Messaging.....	190
8.5	Rollenverteilung.....	191
8.5.1	Application Developer.....	192
8.5.2	Application Owner.....	192
8.5.3	Application Provider.....	193
8.5.4	Supplementary Security Domain Manager	193
8.5.5	Controlling Authority	193
8.5.6	Card Issuer.....	193
8.5.7	Cardholder.....	193
8.5.8	Card Enabler.....	193
8.5.9	Loader.....	194
8.5.10	Card Manufacturer.....	194
8.5.11	IC Manufacturer	194
8.5.12	Platform Owner	194
8.5.13	Platform Developer	194
8.6	OTA Deployment.....	195
8.6.1	Simple Mode	196
8.6.2	Delegated Mode.....	197
8.6.3	Authorized Mode.....	199
8.7	Anforderungen an einen Trusted Service Manager	200
8.7.1	Infrastruktur.....	200
8.7.2	Organisation.....	201

8.7.3	Personal	201
8.7.4	Hardware und Software	202
8.7.5	Netzwerk und Kommunikation	202
	Literatur	203
9	Anwendungen der NFC-Technologie	205
9.1	Das NFC Forum N-Mark	205
9.2	Bezahlen mit NFC	206
9.2.1	Das NFC-Mobiltelefon als Kreditkarte	208
9.2.2	Das NFC-Telefon als Prepaid-Karte	209
9.2.3	Das NFC-Telefon als Debitkarte	211
9.3	Öffentlicher Personennahverkehr	212
9.3.1	Prepaid-Tickets im Secure Element	213
9.3.2	SMS-Tickets ohne Secure Element (Wiener Linien)	214
9.3.3	Postpaid-Modell	215
9.3.4	Die Kredit- oder Bankkarte als Fahrkarte	216
9.3.5	Rhein-Main-Verkehrsverbund (RMV)	216
9.3.6	Deutsche Bahn „Touch and Travel“	218
9.3.7	Hemmnisse und Erfolgsfaktoren	218
9.4	Kino- und Konzertkarten	220
9.4.1	Bestellung der Karten	220
9.4.2	Zustellung und Entwertung der Karten	222
9.5	Zutritt	222
9.5.1	Hotels	223
9.5.2	Firmengebäude	224
9.6	Tourismus-Anwendungen	224
9.7	Produktinformationssystem	225
9.8	Fotos übertragen mit NFC und Bluetooth	226
9.9	McDonald's in Japan	227
9.10	Essensservice für ältere Menschen	228
9.11	Konferenz- und Eventmanagement	231
9.12	Wachdienste	232
9.13	Industrieanwendungen	233
9.14	Medizinische Anwendungen	235
9.14.1	Datenerfassung für die klinische Forschung	235
9.14.2	Öffentliches Gesundheitswesen in Entwicklungsländern	236
9.15	Generische NFC-Plattform	237
	Literatur	240
10	Javaprogrammierung für NFC	243
10.1	JSR 177	243
10.1.1	SATSA-APDU	243
10.1.2	SATSA-JCRMI	244
10.1.3	SATSA-PKI	245
10.1.4	SATSA-CRYPTO	246

10.2	JSR 257	246
10.2.1	Gemeinsame Schnittstelle	247
10.3	PushRegistry und JSR 257	254
10.3.1	NDEF-Records	254
10.3.2	Secure Element Transaktionen	255
10.4	Nokia-Erweiterungen zu JSR 257	255
10.4.1	Peer-to-Peer-Paket	256
10.4.2	PushRegistry	256
10.4.3	Zugriff auf das Secure Element	257
	Literatur	257
	Sachverzeichnis	259