HANSER

Inhaltsverzeichnis

Klaus Schmeh

Elektronische Ausweisdokumente

Grundlagen und Praxisbeispiele

ISBN: 978-3-446-41918-6

Weitere Informationen oder Bestellungen unter

http://www.hanser.de/978-3-446-41918-6

sowie im Buchhandel.

Inhalt

Geleitwort **1**

1 Einführung **1**
1.1 Elektronische Ausweisdokumente 1
1.2 Danksagung und Aufruf zur Mithilfe 5

Teil I: Grundlagen **7**

2 Ausweisdokumente **9**
2.1 Ausweisformate 10
2.2 Welche Ausweisdokumente es gibt 11
2.2.1 Reisepässe 11
2.2.2 Identitätsausweise 15
2.2.3 Ausweise im Gesundheitswesen 17
2.2.4 Behördenausweise 18
2.2.5 Dienstausweise 19
2.2.6 Ausweise im Bildungswesen 19
2.2.7 Mitgliedsausweise 20
2.2.8 Mitarbeiterausweise 20
2.2.9 Kundenausweise 20
2.3 Angriffe auf Ausweisdokumente 21
2.3.1 Totalfälschung 21
2.3.2 Verfälschung 22
2.3.3 Fantasieausweise 22
2.3.4 Fremdnutzung 23
2.3.5 Unrechtmäßiges Erlangen 23
2.3.6 Unbefugtes Auslesen 23
2.3.7 Zerstören 24
2.3.8 Markieren 24

3 Security Engineering ... 25
3.1 Grundlagen des Security Engineering ... 25
3.2 Kryptografie ... 28
3.2.1 Symmetrische Verschlüsselung ... 28
3.2.2 MAC-Funktionen ... 29
3.2.3 Asymmetrische Verschlüsselung ... 30
3.2.4 Digitale Signaturen ... 31
3.2.5 Kryptografische Protokolle ... 33
3.2.6 Public-Key-Infrastrukturen ... 33
3.2.7 Signaturgesetze ... 36
3.3 Authentifizierung ... 36
3.3.1 Nachrichtenauthentifizierung ... 37
3.3.2 Challenge-Response-Verfahren ... 38
3.3.3 Biometrie ... 39
3.4 Evaluierung ... 42

4 Karten- und Mikrochiptechnik ... 45
4.1 Speichertechniken ... 45
4.1.1 Hochprägung ... 45
4.1.2 Maschinenlesbare Schrift ... 46
4.1.3 Strichcodes und 2D-Codes ... 47
4.1.4 Magnetstreifen ... 48
4.1.5 Optischer Speicherstreifen ... 48
4.1.6 Speicherchips ... 49
4.2 Mikrochips und Mikrocontroller ... 49
4.3 Chipkarten und Smartcards ... 50
4.3.1 Kontaktbehaftete Chipkarten ... 52
4.3.2 Kontaktlose Chipkarten ... 53
4.4 Kryptografische Nutzung von Chipkarten ... 56
4.4.1 Wichtige kryptografische Abläufe ... 56
4.4.2 Kryptografische Schnittstellen ... 58
4.5 Smartcard-Betriebssysteme ... 61
4.5.1 Proprietäre Betriebssysteme ... 61
4.5.2 Java Card ... 61
4.5.3 MULTOS ... 62
4.6 Karten-Management ... 63

Teil II: Elektronische Ausweisdokumente ... 65

5 Elektronische Ausweise im Überblick ... 67
5.1 Die Technik elektronischer Ausweise ... 67
5.1.1 Vor- und Nachteile elektronischer Ausweise ... 68
5.1.2 Technische Grundlagen ... 69
5.1.3 Elektronische Ausweise und Biometrie ... 70
5.1.4 Kryptografische Sicherheitsmerkmale ... 71
5.1.5 Elektronische Ausweise als kryptografische Werkzeuge ... 73

5.1.6 Infrastruktur ... 74
5.2 Elektronische Ausweisdokumente im Überblick ... 75
5.2.1 Elektronischer Reisepass ... 75
5.2.2 Elektronischer Identitätsausweis ... 76
5.2.3 Elektronische Ausweise im Gesundheitswesen ... 78
5.2.4 Elektronische Behördenausweise ... 80
5.2.5 Elektronische Dienstausweise ... 80
5.2.6 Elektronische Ausweise im Bildungswesen ... 81
5.2.7 Elektronische Mitgliedsausweise ... 81
5.2.8 Elektronische Mitarbeiterausweise ... 82
5.2.9 Elektronische Kundenausweise ... 82
5.3 Angriffe auf elektronische Ausweise ... 82
5.3.1 Totalfälschung ... 83
5.3.2 Verfälschung ... 83
5.3.3 Fantasieausweise ... 83
5.3.4 Fremdnutzung ... 84
5.3.5 Unrechtmäßiges Erlangen ... 84
5.3.6 Unbefugtes Auslesen ... 84
5.3.7 Zerstören ... 84
5.3.8 Markieren ... 85
5.4 Betriebssysteme für elektronische Ausweise ... 86
5.4.1 Elektronische Ausweise mit proprietären Betriebssystemen ... 86
5.4.2 Elektronische Ausweise mit Java Card ... 86
5.4.3 MULTOS ... 87

6 Elektronische Mitarbeiterausweise ... 89
6.1 Elektronische Mitarbeiterausweise im Überblick ... 89
6.2 Anwendungen elektronischer Mitarbeiterausweise ... 90
6.2.1 Zeiterfassung, Zutrittskontrolle, Bezahlen ... 90
6.2.2 PKI und elektronische Mitarbeiterausweise ... 91
6.2.3 Mitarbeiterausweise als Multiapplikations-Werkzeuge ... 91
6.3 Administration elektronischer Mitarbeiterausweise ... 92
6.4 Kombinierte Mitarbeiter- und Identitätsausweise ... 94

7 Alternative Ansätze ... 95
7.1 Token-Ausweise ... 95
7.2 Implantierte Chips ... 96
7.3 Virtuelle Ausweise ... 97
7.4 Web of Trust ... 99
7.5 Fazit ... 101

Teil III: Standardisierung elektronischer Ausweisdokumente 103

8 Der MRTD-Standard der ICAO 105
8.1 Aufbau des Standards 106
8.2 Kryptografische Schutzmaßnahmen 108
8.2.1 Basic Access Control (BAC) 108
8.2.2 PACE 109
8.2.3 Secure Messaging 110
8.2.4 Passive Authentifizierung 111
8.2.5 Aktive Authentifizierung 111
8.2.6 Chip-Authentifizierung 112
8.2.7 Terminal-Authentifizierung 113
8.2.8 Restricted Identification (RI) 114
8.2.9 EAC 114
8.2.10 mEAC 115
8.3 Kombination der kryptografischen Werkzeuge 115
8.4 MRTD-Implementierungen 116
8.4.1 Golden Reader Tool 116
8.4.2 GlobalTester 118
8.5 Bewertung des MRTD-Standards 118

9 Initiativen für interoperable elektronische Ausweise 119
9.1 Elektronische Reisepässe in der EU 119
9.2 Die European Citizen Card (ECC) 120
9.2.1 Der ECC-Standard 120
9.2.2 Inhalt des Standards 121
9.2.3 Bewertung des ECC-Standards 122
9.3 Die STORK-Initiative 123
9.4 Die Porvoo-Gruppe 123
9.5 Die NETC@RDS-Initiative 124
9.6 Elektronische EHIC 124
9.7 epSOS 125
9.8 E-Ausweis-Abkommen des Golf-Kooperationsrats 126
9.9 Asia IC Card Forum 126
9.10 Fazit 127

10 Die eCard-Strategie der Bundesregierung 129
10.1 Das eCard-Rahmenwerk 129
10.2 Aufbau des eCard-Rahmenwerks 130
10.3 Die vier Schichten des eCard-Rahmenwerks 132
10.3.1 Schicht 1: Application-Layer 132
10.3.2 Schicht 2: Identity-Layer 133
10.3.3 Schicht 3: Service-Access-Layer 134
10.3.4 Schicht 4: Terminal-Layer 135
10.4 Bewertung der eCard-API 136

Teil IV: Beispielprojekte ... 137

11 E-Ausweis-Projekte in Deutschland ... 139
11.1 Elektronischer Personalausweis (ePA) ... 139
11.1.1 Hintergrund des ePA ... 139
11.1.2 Technik des ePA ... 141
11.1.3 Bewertung des ePA ... 143
11.2 Elektronischer Reisepass (ePass) ... 144
11.2.1 MRTD-Reisepass in Deutschland ... 144
11.2.2 Kritik ... 145
11.3 Elektronische Gesundheitskarte (eGK) ... 145
11.3.1 Hintergrund ... 146
11.3.2 Der Vorläufer: Die Versichertenkarte ... 146
11.3.3 Ein weiterer Vorläufer: Die QuaSi-Niere-Karte ... 148
11.3.4 Die elektronische Gesundheitskarte entsteht ... 149
11.3.5 Anwendungen der elektronischen Gesundheitskarte ... 150
11.3.6 Technik der elektronischen Gesundheitskarte ... 152
11.3.7 Der Heilberufsausweis und die Sicherheitsmodulkarte ... 153
11.3.8 Die Telematikinfrastruktur ... 154
11.3.9 Die PKI der elektronischen Gesundheitskarte ... 156
11.3.10 Perspektiven der elektronischen Gesundheitskarte ... 158
11.3.11 Bewertung der elektronischen Gesundheitskarte ... 158
11.4 Elektronischer Dienstausweis (Deutschland) ... 159
11.4.1 Hintergrund ... 159
11.4.2 Technik des eDA ... 160
11.4.3 Bewertung des eDA ... 161
11.5 JobCard (ELENA) ... 161
11.6 ELSTER-Sicherheitsstick ... 162

12 E-Ausweis-Projekte in Österreich ... 163
12.1 Der österreichische elektronische Reisepass ... 163
12.2 Die e-Card ... 164
12.2.1 Hintergrund ... 164
12.2.2 Technik der e-Card ... 165
12.2.3 Bewertung der e-Card ... 166
12.3 Österreichische Bürgerkarte ... 167
12.3.1 Hintergrund der Bürgerkarte ... 168
12.3.2 Technik der Bürgerkarte ... 168
12.3.3 Bewertung der Bürgerkarte ... 169
12.4 Die Educard ... 169
12.4.1 Hintergrund ... 169
12.4.2 Technik der Educard ... 171
12.4.3 Bewertung der Educard ... 171
12.5 Elektronischer Dienstausweis (Österreich) ... 171
12.6 Elektronischer Rechtsanwaltsausweis ... 172

13 E-Ausweis-Projekte in der Schweiz 173
13.1 Der schweizerische elektronische Reisepass 173
13.2 Elektronische Identitätskarte 173
13.3 Elektronische Versichertenkarte 175
13.3.1 Hintergrund der elektronischen Versichertenkarte 175
13.3.2 Technik der elektronischen Versichertenkarte 176
13.3.3 Bewertung der elektronischen Versichertenkarte 177

14 Andere europäische Länder 179
14.1 Europäische Union 179
14.2 Albanien 180
14.3 Belgien 180
14.3.1 Hintergrund der BELPIC 180
14.3.2 Technik der BELPIC 182
14.3.3 Bewertung der BELPIC 182
14.4 Bulgarien 182
14.5 Estland 183
14.5.1 Hintergrund 183
14.5.2 Technik 184
14.5.3 Bewertung der EstEID 185
14.6 Finnland 185
14.6.1 Hintergrund der FINEID 185
14.6.2 Technik der FINEID 186
14.6.3 Bewertung der FINEID 187
14.7 Frankreich 187
14.7.1 Die elektronische Identitätskarte CNIE 187
14.7.2 Die Carte Vitale 189
14.8 Großbritannien 191
14.8.1 Hintergrund der Identity Card 191
14.8.2 Technik der Identity Card 193
14.8.3 Bewertung der Identity Card 193
14.9 Italien 194
14.9.1 Elektronische Identitätskarte 194
14.9.2 Elektronische Gesundheitskarten in Italien 196
14.10 Kroatien 196
14.11 Liechtenstein 197
14.12 Litauen 197
14.13 Montenegro 198
14.14 Niederlande 198
14.15 Polen 198
14.16 Portugal 199
14.16.1 Hintergrund der Cartão de cidadão 199
14.16.2 Technik der Cartão de cidadão 200
14.16.3 Bewertung der Cartão de cidadão 201
14.17 Schweden 201
14.17.1 Hintergrund der nationellt id-kort 201

14.17.2 Technik der nationellt id-kort ... 202
14.17.3 Bewertung der nationellt id-kort ... 203
14.18 Serbien ... 203
14.19 Slowakei ... 204
14.20 Slowenien ... 204
14.20.1 Die slowenische Health Insurance Card (HIC) ... 205
14.20.2 Die slowenische eID ... 207
14.20.3 Der slowenischer elektronische Dienstausweis ... 208
14.21 Spanien ... 208
14.21.1 Hintergrund der DNIe ... 208
14.21.2 Technik der DNIe ... 209
14.21.3 Bewertung der DNIe ... 212
14.22 Tschechien ... 212
14.23 Türkei ... 213
14.24 Ungarn ... 214

15 Ostasien ... 215
15.1 Bangladesch ... 215
15.2 Brunei ... 216
15.3 China ... 216
15.4 Hongkong ... 217
15.4.1 Hintergrund der Smart ID Card ... 217
15.4.2 Technik der Smart ID Card ... 219
15.4.3 Bewertung der Smart ID Card ... 220
15.5 Indien ... 221
15.6 Japan ... 222
15.7 Macao ... 223
15.8 Malaysia ... 223
15.8.1 Hintergrund der MyKad ... 223
15.8.2 Technik der MyKad ... 226
15.8.3 Bewertung von MyKad ... 227
15.9 Singapur ... 228
15.9.1 Hintergrund des SS-ID ... 228
15.9.2 Bewertung des SS-ID ... 230
15.10 Südkorea ... 231
15.11 Thailand ... 231
15.12 Taiwan ... 232

16 Arabien ... 233
16.1 Bahrain ... 234
16.1.1 Hintergrund der bahrainischen Identitätskarte ... 234
16.1.2 Technik der bahrainischen Identitätskarte ... 234
16.1.3 Bewertung der bahrainischen Identitätskarte ... 235
16.2 Jemen ... 235
16.3 Katar ... 236
16.3.1 Hintergrund der ID Card ... 236

16.3.2 Technik der ID Card 236
16.3.3 Bewertung der ID Card 237
16.4 Kuwait 237
16.5 Oman 237
16.5.1 Hintergrund der omanischen Identitätskarte 237
16.5.2 Technik der omanischen Identitätskarte 238
16.5.3 Bewertung der omanischen Identitätskarte 238
16.6 Saudi-Arabien 238
16.6.1 Hintergrund der National ID Card 238
16.6.2 Technik der National ID Card 239
16.6.3 Bewertung der National ID Card 239
16.7 Vereinigte Arabische Emirate 239
16.7.1 Hintergrund der VAE-Identitätskarte 240
16.7.2 Technik der VAE-Identitätskarte 240
16.7.3 Bewertung der VAE-Identitätskarte 240

17 Amerika und Afrika 241
17.1 Brasilien 241
17.2 Ecuador 242
17.3 El Salvador 242
17.4 Guatemala 242
17.5 Marokko 242
17.6 USA 243
17.6.1 PIV-Karte 244
17.6.2 WHTI-Ausweise 245
17.6.3 Common Access Card (CAC) 247
17.6.4 TWIC-Karte 249
17.6.5 Bewertung der elektronischen Ausweise in den USA 250

Anhang 251
Literatur 251
Bildnachweis 257

Register 259