

Andrew Nash  
William Duane  
Celia Joseph  
Derek Brink

# PKI

E-Security implementieren

Übersetzung aus dem  
Amerikanischen von  
Ian Travis



# Inhaltsverzeichnis

<b>Vorwort</b>	<b>15</b>
<b>Über die Autoren</b>	<b>17</b>
<b>Vorwort der Autoren</b>	<b>19</b>
<b>Einführung</b>	<b>21</b>
1.1 Sicherheitstrends	21
1.2 E-Business und Sicherheit heute	22
1.3 Sicherheitsdienste	23
1.4 Public-Key-Infrastructure	26
1.5 Applikationen	27
1.5.1 Leserschaft	28
1.5.2 Über dieses Buch	28
1.6 Über die Autoren	31
<b>Einführung in die Kryptographie</b>	<b>33</b>
2.1 Ist Kryptographie wirklich erforderlich?	34
2.2 Kryptographie	37
2.2.1 Kryptographische Algorithmen	38
2.2.2 Kryptologie und Kryptoanalyse	38
2.2.3 Sicherheit durch Unauffälligkeit	39
2.2.4 Grundkurs Kryptographie	40
2.2.5 Darstellungen	42
2.3 Symmetrische Kryptographie	43
2.3.1 Wählen Sie eine Zahl, eine beliebige Zahl...	44
2.3.2 Zusammenfassung der symmetrischen Kryptographie	52
2.4 Asymmetrische Kryptographie	52
2.4.1 Public- und Private-Keys	56
2.4.2 Die Vor- und Nachteile der asymmetrischen Kryptographie	58
2.4.3 Asymmetrische Kryptographie in der Wiederholung	59
2.5 Das Beste beider Welten	60

2.6	Hashing	64
	Digitale Signaturen	67
2.7		
	Digitale Zertifikate	70
2.8		
	Nicht-Abstreitbarkeit	75
2.9		
	Herzlichen Glückwunsch!	76
2.10		
	Kryptographie in der Wiederholung	77
2.11		
	Absicherung von Web-Transaktionen	77
2.12		
	Warum hat sich die Kryptographie noch nicht überall durchgesetzt?	83
2.13		
	Standardlösungen und Interoperabilität	83
2.13.1		
	Sich die Finger verbrennen	83
2.13.2		
	Migration	84
2.13.3		
	Der Test	86
2.13.4		
		88
	<b>Grundlagen der Public-Key-Infrastructure</b>	
	Grundlagen der Public-Key-Infrastructure	89
3.1		
	Warum die Public-Key-Kryptographie nicht ausreichend ist	89
3.1.1		
	Die Notwendigkeit von vertrauenswürdigen Identitäten	90
3.1.2		
	Zertifizierungsstellen	93
3.1.3		
	Was ist ein digitales Zertifikat?	95
3.1.4		
	Zertifikatstypen und -attribute	96
3.1.5		
	Verwendung von Zertifikaten in Applikationen	102
3.1.6		
	Wozu wird eine Public-Key-Infrastructure benötigt?	104
3.1.7		
	Benutzerauthentifizierung	106
3.1.8		
	Stufen der Authentifizierung	107
3.1.9		
	PKI als Authentifizierungsschema	108
3.1.10		
	Public-Key-Infrastructure-Komponenten	109
3.1.11		
	Life-Cycle-Management für Schlüssel und Zertifikate	111
3.1.12		
	Die Rolle der Autorisierung	115
3.1.13		
	Zusammenfassung	116
3.2		
		122
	<b>PKI-Services und Implementierungen</b>	
	Life-Cycle-Management für Schlüssel und Zertifikate	123
4.1		
	Wie Zertifikate ausgestellt werden	123
4.1.1		
	Wie lange hält ein Schlüssel?	123
4.1.2		
	Zertifikate sperren	131
4.1.3		
	Gültigkeitsprüfung für Zertifikate	134
4M.4		
	Zertifizierungspfade	137
4.1.5		
		138

4.1.6	Schlüsselarten	143
4.1.7	Verteilung von Zertifikaten	147
4.2	Grundlegende Voraussetzungen	151
4.2.1	Schutz von privaten Schlüsseln	152
4.3	Umsetzung von PKI-Services	159
4.3.1	Öffentliche Zertifizierungsstellen	159
4.3.2	Hausinterne Zertifizierungsstellen	163
4.3.3	Unternehmensweite CAs im Outsourcing	164
4.3.4	Entscheidungskriterien	166
4.4	Zusammenfassung	168
	<b>Lebenszyklen der Schlüssel und Zertifikate</b>	171
5.1	Nicht-Abstreitbarkeit und Schlüssel-Management	171
5.1.1	Schlüsselmanagement	173
5.1.2	Generierung von Schlüsseln	173
5.1.3	Keystores	176
5.1.4	Key-Transport	178
5.1.5	Schlüsselarchivierung	179
5.1.6	Schlüsselwiederherstellung	183
5.2	Zertifikat-Management	189
5.2.1	Registrierung von Zertifikaten	190
5.2.2	Teilnehmerzertifikate erneuern	198
5.2.3	CA-Zertifikate erneuern	198
5.2.4	Sperrung von Zertifikaten	199
5.3	Zusammenfassung	214
	<b>Eine PKI-Architektur - das PKIX-Modell</b>	215
6.1	Public-Key-Infrastructure-Architektur	215
6.1.1	Das PKIX-Modell	215
6.1.2	PKIX-Architektur	217
6.1.3	PKIX-Funktionen	219
6.1.4	PKIX-Spezifikationen	222
6.2	PKI-Teilnehmer	225
6.2.1	Registrierungsstelle	225
6.2.2	Zertifizierungsstelle	227
6.2.3	Verzeichnis	227
6.3	PKIX-Management-Protokolle	228
6.3.1	CMP	229

6.3.2	CMC	234
6.4	Nicht-PKIX-konforme Management-Protokolle	238
6.4.1	SCEP	238
6.5	PKIX-Protokolle für die Gültigkeitsprüfung von Zertifikaten	240
6.5.1	OCSP	242
6.5.2	SCVP	244
6.5.3	OCSP-X	245
6.6	Zusammenfassung	247
	<b>Verwendung von PKI in Applikationen</b>	249
7.1	PKI-basierte Dienste	249
7.1.1	Digitale Signatur	249
7.1.2	Authentifizierung	250
7.1.3	Zeitstempel	251
7.1.4	Sicherer Notardienst	252
7.1.5	Nicht-Abstreitbarkeit	252
7.2	PKI-basierte Protokolle	255
7.2.1	Diffie-Hellman-Schlüsselaustausch	255
7.2.2	IPSec	262
7.2.3	S/MIME	267
7.2.4	Time Stamp Protocol	268
7.2.5	WTLS	269
7.3	Formatierungsstandards	269
7.3.1	X.509	270
7.3.2	PKIX	270
7.3.3	IEEE P1363	271
7.3.4	PKCS	271
7.3.5	XML	274
7.4	Application Programming Interfaces	274
7.4.1	Microsoft CryptoAPI	275
7.4.2	Common Data Security Architecture (CDSA)	276
7.4.3	Generic Security Service API	278
7.4.4	Lightweight Directory Access Protocol	278
7.5	Applikationen und PKI-Implementierungen	279
7.6	Applikationen für Datensignaturen	280
7.7	Zusammenfassung	282

	Vertrauensmodelle	283
8.1	Was ist ein Vertrauensmodell?	283
8.1.1	Vertrauen	283
8.1.2	Vertrauensdomänen	284
8.i.3	Vertrauensbasis	286
8.i.4	Vertrauensstellungen	288
8.1.5	Allgemeine hierarchische Organisationen	289
8.2	Vertrauensmodelle	292
8.2.1	Untergeordnete Hierarchie	292
8.2.2	Peer-to-Peer-Modelle	296
8.2.3	Maschenmodelle	301
8.2.4	Hybride Vertrauensmodelle	310
8.3	Wer verwaltet das Vertrauen?	315
8.3.1	Benutzergesteuert	315
8.3.2	Lokale Vertrauenslisten	318
8.3.3	Vertrauen verwalten	320
8.4	Zertifizierungsrichtlinie	322
8.5	Eingeschränkte Vertrauensmodelle	324
8.5.1	Pfadlänge	324
8.5.2	Zertifizierungsrichtlinien	326
8.6	Aufbau und Prüfung der Gültigkeit von Pfaden	330
8.6.1	Pfadaufbau	331
8.6.2	Gültigkeitsprüfung eines Pfades	333
8.7	Implementierungen	334
8.7.1	Identrus-Vertrauensmodell	335
8.7.2	ISO Banking Trust Model	336
8.8	Zusammenfassung	340
	<b>Authentifizierung und PKI</b>	<b>343</b>
9.1	Wer sind Sie?	343
9.1.1	Authentifizierung	343
9.2	Authentifizierung und PKI	345
9.3	Geheimnisse	346
9.4	Passwörter	346
9.4.1	Passwörter im Klartext	347
9.4.2	Daten, die sich aus Passwörtern ableiten lassen	348
9.4.3	Zufällige Elemente hinzufügen	351
9.4.4	Passwortaktualisierungen	356

9.4.5	Und jetzt die Probleme	357
9.4.6	Was Passwörter kosten	360
9.4.7	Passwörter in der Wiederholung	361
9.4.8	Passwörter und PKI	362
9.4.9	Moore's Gesetz hat uns eiskalt erwischt	363
9.4.10	Wie man Passwörter stärkt	364
9.5	Authentifizierungstokens	365
9.5.1	Zweistufige Authentifizierung	367
9.5.2	Authentifizierungstokens	367
9.5.3	PIN-Management	377
9.5.4	Authentifizierungstokens in der Wiederholung	380
9.5.5	Authentifizierungstokens und PKI	381
9.5.6	Tokens als clientseitiger Authentifizierungsmechanismus	382
9.6	Smartcards	384
9.6.1	Aufbau einer Smartcard	385
9.6.2	Wie man sich mit der Smartcard unterhält	386
9.6.3	Smartcard-Klassifizierungen	388
9.6.4	Nicht-kryptographische Smartcards	389
9.6.5	Krypto-Karten	390
9.6.6	Wann ist eine Smartcard keine Smartcard?	392
9.6.7	Applikationen auf der Smartcard	393
9.6.8	Smartcard-Betriebssysteme	394
9.6.9	Manipulationsschutz von Smartcards	395
9.6.10	Widerstandsfähigkeit gegen strukturelle Manipulationen	399
9.6.11	Smartcards in der Wiederholung	402
9.6.12	Smartcards und PKI	403
9.7	Biometrische Authentifizierung	408
9.7.1	Wie die Biometrik funktioniert	408
9.7.2	Biometrische Daten	408
9.7.3	Registrierung	410
9.7.4	FAR/FRR	411
9.7.5	Das Biometrik-Design-Center	411
9.7.6	Probleme mit der Biometrik	413
9.7.7	Eignung	414
9.7.8	Agent-seitiges Spoofing	415
9.7.9	Serverseitige Angriffe	416
9.7.10	Soziale Probleme	418
9.7.11	Cross-System-Replay	419

9.7.12	Sperrung	420
9.7.13	Empfehlungen	421
9.7.14	Der Heilige Gral: Biometrik und PKI	422
9.7.15	Die Biometrik in der Zusammenfassung	424
9.8	Ein Schlusswort zum Thema Authentifizierung	425
	<b>Umsetzung und Betrieb</b>	427
10.0.1	Planung einer PKI	427
10.0.2	Bestimmende Faktoren im Unternehmen	427
10.0.3	Planung der Applikationen	430
10.0.4	Planung der Architektur	431
10.0.5	Entscheidungen	435
10.0.6	Auswirkung auf die Benutzer	435
10.0.7	Support und Administration	437
10.0.8	Auswirkungen auf die Infrastruktur	438
10.0.9	Planung der Zertifikatinhalte	440
10.0.10	Datenbanken integrieren	443
10.0.11	Rechtliche Überlegungen und Richtlinien	444
10.0.12	Vertrauens modeile	449
10.1	Überlegungen zur Umsetzung	456
10.2	Überlegungen zum Betrieb der PKI	458
10.3	Zusammenfassung	461
	<b>PKI und Return-On-Investment</b>	463
11.1	Total-Cost-of-Ownership - Das »I« in ROI	464
11.1.1	Produkte/Technologien	465
11.1.2	Standorte und Räumlichkeiten	467
11.1.3	Menschen	467
11.1.4	Prozesse	467
11.1.5	Total-Cost-of-Ownership: Zusammenfassung	468
11.2	Rendite: Das »R« in ROI	468
11.2.1	Geschäftsprozesse	470
11.2.2	Bemessungskriterien	475
11.2.3	Umsätze	475
11.2.4	Kosten	479
11.2.5	Einhaltung von Bestimmungen	482
11.2.6	Risiken	483
11.2.7	Rendite: Zusammenfassung	485



11.3	PKI-ROI: Zusammenfassung	486
11.4	Referenzen	487
	<b>X.509-Zertifikate</b>	489
A.1	Zertifikattypen	489
A.2	Zertifikatformat	490
A.3	Zertifikaterweiterungen	493
A.3.1	Statusindikator kritisch/nicht kritisch	493
A.3.2	Schlüsselerweiterungen	494
A.3.3	Richtlinienerweiterungen	497
A.3.4	Erweiterte Teilnehmer- und Ausstellerinformationen	499
A.3.5	CertificationPathConstraint-Erweiterungen	500
A.4	Format der Sperreintragsliste (Certificate Revocation List - CRL)	502
A.4.1	Erweiterungen der CRL und der CRL-Einträge	504
A.5	CRL-Verteilungspunkte und Delta-CRL-Erweiterungen	509
A.5.1	Zertifikaterweiterungen	510
A.5.2	CRL-Erweiterungen	511
A.5.3	CRL-Eintragserweiterungen	512
	<b>Lösungen</b>	515
B.1	Die Antwort	515
B.2	Die Belohnung	520
B.2.1	Der Boden	521
B.2.2	Die Füllung	521
	<b>Privilege-Management-Infrastruktur</b>	523
C.1	Attributzertifikate	524
C.1.1	Die Beweggründe	524
C.1.2	Attribute	525
C.1.3	Format des Attributzertifikats	525
C.2	Privilege-Management-Infrastruktur	528
C.2.1	Attribute Authority	528
C.2.2	Autoritätsursprung	529
C.2.3	Attributzertifikat-Sperreintragslisten	529
C.3	PMI-Modelle	529
C.3.1	Privilege-Management-Modell	529
C.3.2	Delegierungsmodell	531
C.3.3	Rollenmodell	532

C.3.4	Akquisitionsmodell für Attributzertifikate	534
C.4	Privilege-Management-Zertifikaterweiterungen	534
C.4.1	Grundlegende Privilege-Management-Erweiterungen	535
C.4.2	Sperrung von Privilegien	536
C.4.3	Autoritätsursprung	536
C.4.4	Rollenerweiterung	537
C.4.5	Erweiterung der Delegierung	538
C-5	PKIX	539
C.6	Zusammenfassung	540
	<b>Glossar</b>	<b>543</b>
	<b>Stichwortverzeichnis</b>	<b>553</b>