

Contents

1	The Purpose of PKI	1
1.1	The Internet	1
1.2	Security Goals	2
1.2.1	Confidentiality	2
1.2.2	Integrity	3
1.2.3	Entity Authentication	3
1.2.4	Data Authenticity	4
1.2.5	Non-repudiation	5
1.2.6	Other Security Goals	5
1.3	Cryptography	5
1.3.1	Secret Key Encryption	5
1.3.2	Public Key Encryption	7
1.3.3	The RSA Public Key Cryptosystem	8
1.3.4	Other Public Key Cryptosystems	9
1.3.5	Hybrid Encryption	10
1.3.6	Cryptographic Hash Functions and Message Authentication Codes	11
1.3.7	Digital Signatures	12
1.3.8	The RSA Signature Scheme	13
1.3.9	Other Digital Signature Schemes	14
1.4	Why Public Key Infrastructure?	15
1.5	Identity-Based Public Key Cryptography	16
1.6	Object Identifiers	17
1.7	Exercises	17
	References	18
2	Certificates	21
2.1	The Concept of a Certificate	21
2.2	X.509 Certificates	22
2.2.1	Structure	22
2.2.2	tbbsCertificate	24

2.2.3	signatureAlgorithm	27
2.2.4	signatureValue	27
2.3	X.509 Certificate Extensions	27
2.4	Attribute Certificates	31
2.5	CV Certificates	31
2.6	PGP Certificates	33
2.7	Other Certificates	33
2.7.1	WAP Certificates	34
2.7.2	SPKI Certificates	34
2.7.3	Traceable Anonymous Certificate	35
2.8	Exercises	35
	References	37
3	Trust Models	39
3.1	Direct Trust	39
3.2	Web of Trust	42
3.2.1	Key Ring	44
3.2.2	Trust Signatures	47
3.2.3	Probabilistic Trust Model for GnuPG	48
3.3	Hierarchical Trust	48
3.3.1	Basic Constraints	50
3.4	Combining Trust Hierarchies	51
3.4.1	Trusted Lists	52
3.4.2	Common Root	53
3.4.3	Cross-Certification	56
3.4.4	Bridge	56
3.5	Exercises	58
	References	60
4	Private Keys	61
4.1	Private Key Life Cycle	61
4.2	Personal Security Environments	62
4.3	Software PSEs	63
4.3.1	PKCS#12	63
4.3.2	PKCS#8	64
4.3.3	Java KeyStore	65
4.3.4	Application-Specific Formats	65
4.4	Hardware PSEs	68
4.4.1	Smart Cards	68
4.4.2	Smart Card Readers	69
4.4.3	Smart Card Communication Interfaces	70
4.4.4	Hardware Security Module	72
4.5	Exercises	73
	References	73

5	Revocation	75
5.1	Requirements	75
5.2	Certificate Revocation Lists	76
5.2.1	Basic Fields	76
5.2.2	CRL Extensions	79
5.2.3	Issuing Time of a CRL	81
5.2.4	Delta CRLs	82
5.2.5	Authority Revocation List	83
5.2.6	Indirect CRLs	83
5.3	Certificate Extensions Related to Revocation	83
5.3.1	CRL Distribution Points	83
5.4	OCSP	84
5.4.1	Functionality	84
5.4.2	Extensions	86
5.4.3	Lightweight OCSP	89
5.4.4	Design of an OCSP Server	89
5.5	Other Revocation Mechanisms	89
5.5.1	Novomodo	89
5.5.2	Short-Lived Certificates	90
5.6	Revocation in PGP	90
5.7	Exercises	91
	References	94
6	Validity Models	95
6.1	The Shell Model	95
6.2	The Chain Model	97
6.3	The Modified Shell Model	98
6.4	Exercises	100
	References	101
7	Certification Service Provider	103
7.1	Certificate Life Cycle	103
7.1.1	Certificate Generation Phase	103
7.1.2	Certificate Validity Phase	104
7.1.3	Certificate Invalidity Phase	104
7.2	Registration Authority	105
7.3	Certification Authority	107
7.4	Other Components	108
7.5	Communication Within CSPs	108
7.5.1	Cryptographic Protection of Messages	108
7.5.2	Certificate Requests	109
7.5.3	Complex Message Formats and Protocols	112
7.6	Exercises	115
	References	115

8	Certificate Policies	117
8.1	Structure of Certificate Policies	117
8.1.1	Certification Practice Statement	119
8.2	Relevant Certificate Extensions	119
8.2.1	Certificate Policies	119
8.2.2	Policy Mappings	119
8.2.3	Policy Constraints	121
8.2.4	Inhibit anyPolicy	121
8.3	Extended Validation Certificates	122
8.4	Exercises	122
	References	123
9	Certification Paths: Retrieval and Validation	125
9.1	LDAP	125
9.1.1	Storing Certificates	126
9.1.2	Certificate Search	129
9.1.3	Storing CRLs	130
9.1.4	Security	131
9.2	Other Certificate Retrieval Methods	131
9.2.1	DNS	131
9.2.2	HTTP	132
9.2.3	Web Servers and FTP Servers	132
9.2.4	WebDAV	132
9.3	Certification Path Building	132
9.4	Certification Path Validation	134
9.4.1	Validation Algorithm	135
9.5	Server-Based Certificate Validation Protocol (SCVP)	137
9.6	Relevant Certificate Extensions	138
9.6.1	Authority Information Access	138
9.6.2	Subject Information Access	139
9.7	Exercises	140
	References	141
10	PKI in Practice	143
10.1	Internet	143
10.2	Email	144
10.2.1	S/MIME	145
10.2.2	PGP	147
10.3	Code Signing	152
10.4	VPN	154
10.5	Legally Binding Electronic Signatures	156
10.6	E-Government	159
10.7	Exercises	162
	References	163

Contents	xi
A Basic Path Validation Algorithm.....	165
Solutions to the Exercises	173
Index	187