

Index

- ABA Digital Signature Guidelines*, 185
- AC, 59, 60, 82
- Access control list (ACL), 59
- Accreditation certificate, 137
- ACL, 59
- Adleman, Len, 17
- Administrators, 277
- Advanced Encryption Standard (AES), 9
- AES, 9
- AIA private extension, 78, 163
- Algorithms
 - CAST-128, 9, 45
 - DH, 18
 - DSA, 17–18
 - ECDH, 18
 - ECDSA, 18
 - ongoing work, 19
 - RSA, 17
 - SHA-1, 18–19
- Alternative certificate formats, 78–82
- Anonymous certificate, 56, 166
- Anonyms, 56
- ANSI X9F, 227
- ANX, 245
- Application enabler, 22
- Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 7
- Asymmetric cipher model, 13
- Asymmetric ciphers, 12
- Attribute certificate (AC), 59, 60, 82
- Auditable delegation, 55
- Authentication, 37–44
- Authentication without identification, 57
- Authority Information Access (AIA), 78, 163
- Authority Key Identifier, 74, 111, 246
- Authorization, 54
- Authorization authorities, 54–55
- Automatic key update, 30–31
- Automotive Network eXchange (ANX), 245
- Backup, 97, 98
- Backup facility, 97
- Barriers to deployment, 283–286
- Base Update, 113
- Basic Constraints, 76
- Bibliography, 297–309
- Bilateral cross-certification, 193
- Blinded delegation, 55
- Book, overview, 3–5
- Books. *See* Further reading

- Boolean expressions, 59
- Border repository, 167–168
- Bridge CA, 193, 245–246, 292–293
- Bridge repository, 168
- BTP, 231
- Build vs. buy, 270
- Business case considerations, 263–265
- Business drivers, 27–28
- Business models, 287–294
 - external communications models, 288–290
 - factors to consider, 291
 - government-sponsored initiatives, 291–292
 - interdomain trust, 292–293
 - internal communications models, 287–288
 - internal/external hybrids, 290–291
- Business-to-business communication, 289
- Business-to-business trust relationship, 292–293
- Business-to-consumer communication, 290
- Business Transaction Processing (BTP), 231
- CA, 28–29, 85–86
 - loose hierarchy, 134–135
 - responsibilities, 188–189, 191
 - strict hierarchy, 132–134
- CA-CA Interoperability, 137
- CA certificates, 71
- CA Interoperability Pilot (Phase I)*, 248
- CARL, 179–180
- CAST-128, 9, 45
- Certificate authority, 85
- Certificate creation, 94–95
- Certificate dissemination, 96. *See also* PKI
 - information dissemination
- Certificate expiration, 101
- Certificate extension, 74–78
- Certificate Issuer, 110
- Certificate Management messages over CMS (CMC), 254
- Certificate path processing, 146–149
- Certificate perishability, 76
- Certificate policies, 75, 82–85
- Certificate policy/certification practices
 - framework, 241
- Certificate renewal, 101, 102
- Certificate repository, 29
- Certificate retrieval, 97–98
- Certificate revocation, 29–30, 101–102, 105–129
 - CARL, 114–115
 - complete CRL, 114
 - CRL, 107–113
 - CRL distribution points, 115–116
 - CRT, 120–122
 - Delta CRL, 118–119
 - EPRL, 115
 - indirect CRL, 119–120
 - indirect Delta CRL, 119
 - OCSP, 122–125
 - on-line query mechanisms, 122
 - other options, 126
 - overview (table), 128–129
 - performance, 127
 - periodic publication mechanisms, 107–125
 - redirect CRL, 116–118
 - scalability, 127
 - SCVP, 125
 - short-lived certificates, 126
 - terminology, 107
 - timelines, 127
 - updating/posting information, 106
- Certificate revocation list. *See* CRL
- Certificate revocation model, 106
- Certificate revocation sample scenarios, 102
- Certificate revocation tree (CRT), 120–122, 129
- Certificate trust list (CTL), 137
- Certificate update, 31, 101, 102
- Certificate validation, 98–99
- Certificates and certification, 69–87
 - AC, 82
 - alternative formats, 78–82
 - certificate policies, 82–85
 - certification authority. *See* CA
 - digital certificate, 71–72
 - extensions, 74–78
 - perishability, 76
 - PGP, 80
 - private extensions, 78
 - registration authority, 86–87

- SET, 81–82
- SPKI, 79–80
 - structure/semantics, 72–78
 - types of certificates, 70, 78–82
- Certification, 85
- Certification authority. *See* CA
- “Certification Authority Interoperability: From Concept to Reality—Results of the NACHA Internet Council CA Interoperability Pilot,” 249
- Certification authority revocation list (CARL), 114–115, 128, 179–180
- Certification practice statement (CPS), 82–84
- Certification practice statement (CPS) qualifier, 75
- Cipher, 8
- Ciphertext, 8
- Client-side PKI software, 171–173
- Client software, 33–35
- Closed environment, 272
- CMC, 254
- CMP, 95
- Complete CRLs, 114
- Comprehensive PKI, 63
- Comprehensive security, 26–27
- “Computer Crime and Security Survey,” 264
- Confidentiality, 43, 45, 194
- Core PKI services, 37–48
 - authentication, 37–44
 - commonality of underlying algorithms, 47
 - confidentiality, 43, 45
 - entity naming, 47
 - integrity, 42–45
 - mechanisms, 43–45
 - on-line vs. off-line operations, 46–47
 - operational considerations, 45–47
 - performance, 46
- Corporate-level acceptance, 286
- Cost considerations, 265–266
- CPS, 82–84
- CPS qualifier, 75
- Criticality flag, 74
- CRL, 107–113, 128
 - per-CRL extensions, 111–113
 - per-entry extensions, 110–111
 - private extensions, 113
 - versions, 108–110
- CRL Distribution Point, 74–75, 115–116, 128
- CRL Number, 111
- CRL profiles, 108
- CRL Scope, 112
- CRL Stream Identifier, 112
- CRMF, 95
- Cross-certification, 32, 143–145
- Cross-recognition, 137
- Cryptographic hash function, 16
- Cryptography: Theory and Practice*, 7
- Cryptography and Network Security: Principles and Practices*, 7
- CTL, 137
- DAP, 167, 283
- Data certification server protocols, 241
- Data Encryption Standard (DES), 9
- Data integrity, 16, 42–45
- Data origin identification, 38
- Data Validation and Certification Server Protocols (DVCS), 255
- Decryption, 8
- Decryption private key, 93
- Delegated path discovery (DPD), 125
- Delegated path validation (DPV), 125
- Delegation, 55
- Delta CRL, 118–119, 128
- Delta CRL Indicator, 113
- Delta Information, 112
- Deployment considerations, 259–296
 - barriers to deployment, 283–286
 - build vs. buy, 272
 - business case considerations, 263–265
 - business models, 287–294.
 - See also* Business models
 - certificate revocation, 277–278
 - closed vs. open environment, 272–273
 - cost considerations, 265–266
 - disaster planning/recovery, 279
 - end-entity roaming, 278
 - facility requirements, 277
 - factors to consider, 296

- further reading, 296
- hierarchical vs. distributed models, 270
- in-sourcing vs. out-sourcing, 271–272
- interoperability considerations, 274–275
- key recovery, 278–279
- keys to success, 295
- mitigating risk, 280
- on-line vs. off-line operations, 276
- peripheral support, 276
- personnel requirements, 277
- PKI pilots, 267
- repository issues, 279, 283–284
- security assurance, 279–280
- standard vs. proprietary solutions, 274
- targeted applications vs. comprehensive solution, 274
- vendor selection, 280
- X.509 vs. alternative certificate format, 273
- DES, 9
- Design considerations, 269–281.
 - See also* Deployment considerations
- DH, 18
- DH communication configurations, 46
- DH key pair, 152
- Diffie, Whitfield, 11
- Diffie-Hellman algorithm, 18
- Diffie-Hellman (DH) key pair, 152
- Diffie-Hellman paper, 11
- Digital certificate, 71–72
- Digital signature, 14–16, 44, 71, 185
- Digital Signature Algorithm (DSA), 17–18
- Digital Signature Guidelines*, 185
- Directory Access Protocol (DAP), 167, 283
- Directory Information Shadowing Protocol (DISP), 168, 284
- Directory information tree (DIT), 165
- Disaster preparation/recovery, 179–182
- DISP, 168, 284
- Dissemination of information. *See* PKI information dissemination
- Distinguished name (DN), 73, 146, 165
- Distributed trust architecture, 135–138
- Distributed vs. hierarchical models, 270
- DIT, 165
- DN, 73, 146, 165
- DNS, 284
- DNS SRV records, 163
- Domain name system (DNS), 284
- DPD, 125
- DPV, 125
- DSA, 17–18
- DVCS, 255
- E-mail composition (laptop computer), 173
- E-Sign legislation, 183–184
- ebXML, 231
- ECDH, 18
- ECDSA, 18
- ECOM, 234
- EDIFACT, 230
- EEMA PKI Challenge, 250
- EESSI, 235
- Electric power infrastructure, 21
- Electronic business XML (ebXML), 231
- Electronic Commerce Promotion Council of Japan (ECOM), 234
- Electronic communications infrastructure, 21
- Electronic medical record (EMR), 291
- Electronic signature, 185
- Electronic Signature Directive, 186–187
- Electronic signature legislation, 183–188
- Electronic Signature Testsuite for Inter-Operability (ESTIO), 235
- Electronic Signatures in Global and National Commerce Act (E-Sign), 183–184
- ElGamal, 18
- Elliptic curve DH (ECDH), 18
- Elliptic curve DSA (ECDSA), 18
- EMR, 291
- Encapsulating Security Payload, 167
- Encryption, 8, 14
- Encryption certificate, 93
- End entity, 132
- End-entity certificates, 71
- End-entity initialization scenario, 91
- End-entity public-key certificate revocation list (EPRL), 115, 128
- End-entity registration, 91–92
- End-entity roaming, 278
- End-user transparency, 26

- End users, 132
- Enterprise secure e-mail, 64–66
- Entity identification, 37–39
- Entity naming, 47, 145–146, 198
- Ephemeral-ephemeral DH, 46
- Ephemeral-static DH, 46
- EPRL, 115, 128
- ESTIO, 235
- EU Electronic Signature Directive, 186–187
- European Electronic Signature Standardization Initiative (EESSI), 235
- European Forum for Electronic Business (EEMA), 250
- Extended key usage, 74
- eXtensible Access Control Markup Language (XACML), 59, 231
- Extensions, 74–78
- External communications business model, 288–290
- Extranet security, 64, 65
- Facility requirements, 277
- Federal Information Processing Standard (FIPS) 140–1, 94
- Federal Public-Key Infrastructure (FPKI), 232
- Federal Public Key Infrastructure Certificate and CRL Extensions Profile*, 247
- Fingerprint, 134
- FIPS 140–1, 94
- Forward cross-certificate, 143
- Four-corner trust model, 138–139, 248
- FPKI, 232
- Freshest CRL, 113
- Freshest CRL Pointer, 77–78
- Further reading. *See also* Web sites
 - bibliography, 297–309
 - certificate/CRL storage and retrieval, 254–256
 - certificate/CRL syntax, 253–254
 - deployment issues, 296
 - interoperability initiatives, 256–257
 - life-cycle management protocols, 253–254
 - PKI, generally, 218
 - standards, 253–258
 - XML-based initiatives, 256
- Future of PKI, 207–216
- Generic digital signature process, 15
- Generic Security Service Application Program Interface (GSS-API), 240
- GOC PKI, 232–233, 270
- GOL initiative, 294
- Government of Canada Public-Key Infrastructure (GOC PKI), 232–233
- Government On-Line (GOL) initiative, 294
- Government-sponsored initiatives, 291–292
- GSS-API, 240
- GTE CyberTrust/Baltimore Technologies
 - OmniRoot, 293
- Handbook of Applied Cryptography*, 7
- Handshaking protocols, 47
- Hardware components, 175
- Hash algorithms, 18–19
- Health Information Portability and Accountability Act (HIPAA), 291
- Hellman, Martin, 11
- Hierarchical vs. distributed models, 270
- Hierarchy
 - loose, 134–135
 - policy-based, 135
 - strict, 132–134
 - trusted-issuer, 134
- HIPAA, 291
- Hold Instruction Code, 110, 111n
- Hub-and-spoke configuration, 138
- ICE-CAR, 234–235
- Identification, 57, 198
- Identifier, 198
- Identity, 145
- Identity mapping, 62
- Identity uniqueness, 145
- Identrus, 292
- IDUP-GSS-API, 240
- IEEE, 230
- IEEE P1363, 230
- IEEE P1363a, 230
- IETF, 224

- IETF PKIX Working Group, 224–225, 238, 249, 255
- IKE, 228
- In-band protocol distribution, 96
- In-band protocol exchange, 169
- In-sourcing, 271
- Independent certificate management, 155–156
- Independent Data Unit Protection specification (IDUP-GSS-API), 240
- Indexical reference problem, 57
- Indirect CRLs, 119–120, 128
- Indirect Delta CRLs, 119, 128
- Information dissemination.
 - See* PKI information dissemination
- Infrastructure, 171
- Inhibit Any Policy, 77
- Inhibit Policy Mapping, 77
- Institute of Electrical and Electronics Engineers (IEEE), 230
- Integrity, 42–45
- Inter-enterprise-signed transactions, 66
- Interdomain cross-certification, 143
- Interdomain replication, 168–169
- Interdomain repository deployment options, 167
- Interdomain trust, 292–293
- Intermediate CAs, 132
- Intermediate repository, 166
- Internal communications business model, 287–288
- Internal/external business model hybrids, 290–291
- Internet Engineering Task Force (IETF), 224
- Internet Key Exchange (IKE), 228
- Internet PKI (IPKI), 64, 224
- Internet web sites. *See* Web sites
- Internet X.509 Certificate Request Message Format (CRMF), 95
- Internet X.509 Public Key Infrastructure Certificate Management Protocols (CMP), 95
- Interoperability considerations, 274–275
- Interoperability initiatives, 245–250
- Interoperability testing, 244–245
- Interworking Public Key Certification Infrastructure for Commerce, Administration and Research (ICE-CAR), 234–235
- Intradomain cross-certification, 143
- Invalidation Date, 111
- IPKI, 64, 224
- IPsec, 228, 239
- ISO TC68, 226
- Issuer, 73, 109
- Issuer Alternative Name, 76, 111
- Issuer Unique ID, 73
- Issuing Distribution Point, 112–113
- Java Community Process (JCP), 234
- Java Specification Requests (JSRs), 234
- KDC, 9
- Kennedy-Kassebaum Bill, 291
- Kerberos, 59, 60
- Key, 8
 - Key agreement, 17
 - Key and certificate history, 31
 - Key archive, 103, 104
 - Key backup, 97, 98
 - Key backup and recovery, 30
 - Key/certificate distribution, 95
 - Key/certificate life-cycle management, 89–104
 - cancellation phase, 100–104
 - certificate creation, 94–95
 - certificate dissemination, 96. *See also* PKI information dissemination
 - certificate expiration, 101
 - certificate retrieval, 97–98
 - certificate revocation, 101–102.
 - See also* Certificate revocation
 - certificate validation, 98–99
 - end entity registration, 91–92
 - initialization phase, 91–97
 - issued phase, 97–100
 - key archive, 104
 - key backup, 97
 - key/certificate distribution, 95
 - key history, 103

- key pair generation, 92–94
- key recovery, 99
- key update, 100
- underlying assumptions, 90
- Key compromise, 176–178
- Key distribution center (KDC), 9
- Key escrow, 98
- Key establishments, 16–17
- Key exchange, 90n
- Key history, 31–32, 103
- Key management, 90n
- Key pair, 12
- Key pair generation, 92–94
- Key pair uses, 152–153
- Key recovery, 99
- Key transfer, 16
- Key update, 31, 100
- Key usage, 74
- Launching a PKI deployment.
 - See* Deployment considerations
- LDAP, 226
- LDAP data interchange format (LDIF), 169
- LDAP Duplication/Replication/Update Protocols (LDUP) Working Group, 161, 169, 284
- LDAPext Working Group, 226, 284
- LDAPv2, 161, 226, 238
- LDAPv3, 161, 226, 238
- LDIF, 169
- LDUP Working Group, 161, 169, 284
- Legal issues, 183–194
 - CA responsibilities, 190–191
 - confidentiality, 194
 - Digital Signature Guidelines*, 185
 - E-Sign, 183–184
 - EU Directive, 186–187
 - other contractual-based frameworks, 193
 - private enterprise PKIs, 192–193
 - relying party responsibilities, 191–192
 - subscriber responsibilities, 190–191
- Life-cycle management. *See* Key/certificate life-cycle management
- Lightweight Directory Access Protocol (LDAP), 226
- Lightweight Directory Access Protocol (LDAP) Version 2 (LDAPv2), 161, 226, 238
- Lightweight Directory Access Protocol (LDAP) Version 3 (LDAPv3), 161, 226, 238
- “Limits to the Scale of a Public Key Infrastructure,” 127
- Local authentication, 38
- Local registration authorities (LRAs), 86
- Logging-in, 23
- Loose hierarchy of certification authorities, 134–135
- LRAs, 86
- MAC, 15, 44
- Medical Records Confidentiality Act, 291
- Mesh configuration, 137
- Message authentication code (MAC), 15, 44
- Minimum interoperability specification, 247–248
- “Minimum Interoperability Specification for PKI Components, Version 1,” 247
- “Minimum Interoperability Specification for PKI Components, Version 2—Second Draft,” 247–248
- Minimum Interoperability Specifications for PKI Components (MISPC), 232
- Minimum-knowledge, 17
- MISPC, 232
- “Model of Certificate Revocation, A,” 127
- Multifactor authentication, 39
- Multiple certificates per entry, 151–157
 - independent certificate management, 155–156
 - key pair uses, 152–155
 - multiple key pairs, 151–152
 - real-word difficulties, 155
 - support for non-repudiation, 156–157
- Multiple key pairs, 151–152
- Multiple keys per user, 153
- Multivendor interoperability, 284
- Mutual cross-certification, 143, 144

- Name, 198
- Name Constraints, 77, 145
- Naming entities, 47, 145–146, 198
- National Automated Clearing House Association (NACHA), 248
- Negotiation (“handshaking”) protocols, 47
- “New Directions in Cryptography” (Diffie/Hellman), 11
- Next Update, 110
- No action, 101
- Non-repudiation, 32–33
 - complexity, 53
 - connection with other services, 52
 - defined, 51
 - human factor, 53
 - secure data archive, 52
 - support for, 93, 156–157
 - variants, 51
- Non-repudiation of origin, 51
- Non-repudiation of receipt, 51
- Nonblinded delegation, 55
- Noncritical extension, 74
- Notarization, 50–51

- OASIS, 231
- Object identifiers (OID), 73n, 83, 85
- OCSP component interaction, 123
- OCSP request, 123
- OCSP responder, 122
- Off-line operations, 173–174, 276
- Off-line vs. on-line operations, 46–47
- Offloading PKI-related processing, 241
- OID, 73n, 83, 85
- OmniRoot, 293
- On-line operation, 276
- On-line query mechanisms, 122
- On-line vs. off-line operations, 46–47
- Ongoing standardization work, 240–241
- Online Certificate Status Protocol (OCSP), 122–125, 128
- Open environment, 273
- Open Mobile Alliance, 230
- OpenPGP, 80, 160, 229–230
- Operational considerations. *See* PKI
 - operational considerations
- Operators, 277
- Ordered List, 112
- Organization for the Advancement of Structured Information Standards (OASIS), 231
- Out-of-band distribution, 96
- Out-sourcing, 271
- Overview of book, 3–5

- P1363, 230
- Partitioned CRLs, 115
- Path construction, 147–148
- Path Length Constraints, 76–77, 145
- Path validation, 148
- PEM, 134n
- Performance, 284
- Periodic publication mechanisms, 107–125
- Peripheral support, 276
- Personnel requirements, 277
- Pervasive substrate, 21–22
- PGP, 80, 142, 160, 229
- Physical security, 174–175
- Physically secure archive facilities, 62
- PKCS 7/10, 95
- PKI. *See* Public-key infrastructure (PKI)
- PKI-aware software, 285–286
- PKI certificate revocation. *See* Certificate revocation
- PKI Challenge, 250
- PKI deployment. *See* Deployment considerations
- PKI disaster scenarios, 179–182
- PKI disclosure statement, 84
- PKI-enabled applications, 285–286
- PKI-enabled services, 49–67
 - comprehensive PKI/current practice, 63–67
 - non-repudiation, 51–53
 - notarization, 50–51
 - operational considerations, 61–63
 - privacy, 56–58
 - privilege management, 53–56
 - required mechanisms, 58–60
 - secure communication, 49
 - secure time stamping, 50

- PKI information dissemination, 96, 159–170
 - in-band protocol exchange, 169
 - private dissemination, 159–160
 - repository. *See* Repository
- PKI interoperability, 245–250
- PKI networking, 136
- PKI notary, 51
- PKI operational considerations, 171–182
 - client-side software, 171–173
 - disaster preparation/recovery, 179–182
 - hardware components, 175
 - off-line operations, 173–174
 - physical security, 174–175
 - user key compromise, 176–178
- PKI pilots, 267
- PKI-TWG, 247
- PKI-usage scenarios, 64–67
- PKI X.509, 249
- PKIX Working Group, 224–225, 238, 249, 255
- Plaintext, 8
- PMI, 59, 240–241
- Policy authorities, 85
- Policy constraints, 77, 145
- Policy decision point (PDP), 59
- Policy management authorities, 85
- Policy Mappings, 75
- Policy qualifiers, 75
- Policy server schemes, 60
- Power-of-attorney delegation, 55
- Pretty Good Privacy (PGP), 80, 142, 160, 229
- Privacy, 56–58
- Privacy architecture, 60
- Privacy certificates, 62
- Privacy Enhanced Mail (PEM), 134n
- Private dissemination, 159–160
- Private enterprise PKIs, 192–193
- Private extensions, 78
- Private key, 12n
- Private Key Usage Period, 75
- Privilege management, 53–56
- Privilege management infrastructure (PMI), 59, 240–241
- Privilege management infrastructure mechanisms, 59–60
- Privilege policy creation mechanism, 58–59
- Privilege policy processing engines, 59
- Profile, 244
- Protocols for digital notary services, 241
- Provisioning Services Markup Language (PSML), 231
- Proxy, 166
- Pseudonymous certificate, 56
- Pseudonymous privacy, 62
- Pseudonyms, 56
- PSML, 231
- Public-key algorithms. *See* Algorithms
- Public-key certificate, 85. *See also* Certificates and certification
- Public-key cryptography, 12
- Public-key infrastructure (PKI), 217
 - automatic key update, 30–31
 - benefits/costs, 263–268
 - certificate authority, 28–29
 - certificate repository, 29
 - certificate revocation, 29–30
 - client software, 33
 - cross-certification, 32
 - deployment. *See* Deployment considerations
 - further reading, 218
 - future of, 207–216
 - key backup and recovery, 30
 - key history, 31–32
 - non-repudiation, 32–33
 - pilots, 267
 - real-life scenario, 203–206
 - simple definition, 28
 - time stamping, 33, 50
 - value of, 200–203
 - what does PKI do/not do, 196–200
- Public Key Infrastructure Technical Working Group (PKI-TWG), 247
- Publication, 160
- RA, 86–87
- Real-life scenario, 203–206
- Reason Code, 110

- Redirect CRLs, 116–118, 128
- Reduced sign-on, 25n
- References. *See* Further reading, Web sites
- Registration authority (RA), 86–87
- Relying party responsibilities, 191–192
- Remote authentication, 38
- Repository
 - advantages/disadvantages, 163–165
 - border, 167–168
 - defined, 161
 - deployment issues, 279, 283–284
 - direct access, 166–167
 - interdomain issues, 165–169
 - interdomain replication, 168–169
 - locating, 162–163
 - performance considerations, 164
 - shared, 168
 - types, 162
- Repudiation, 33
- Require Explicit Policy, 77
- Reverse cross-certificate, 143
- Revocation. *See* Certificate revocation
- Revoked Certificates, 110
- RFC2459, 72
- RFC2559, 255
- RFC2585, 255
- RFC2587, 255
- RFC3280, 72, 108
- Rivest, Ron, 17, 19
- Roaming, 278
- Rollover, 154
- Root CA, 132
- ROT-13, 9
- RSA, 17

- S/MIME, 227, 238–239
- S/MIMEv3 specifications, 227
- SAML, 59, 231
- SASI, 241
- Scalability, 284
- SCVP, 125, 255
- Secret key, 12n
- Secure communication, 49
- Secure e-mail, 49

- Secure Electronic MarketPlace, EuRope (SEMPER), 233
- Secure Electronic Transaction (SET), 81–82, 180, 233
- Secure hash algorithm (SHA-1), 18–19
- Secure MIME (S/MIME), 227, 238–239
- Secure protocols, 61
- Secure sign-on, 23–25
- Secure time stamping, 33, 50
- Secure time-stamping protocols, 241
- Secure VPN, 49
- Secure Web server access, 49
- Securities Industry Root CA (SIRCA) proof of concept, 250
- Security Assertion Markup Language (SAML), 59, 231
- Security assurance, 279–280
- Security infrastructure, 21–22
- Security officers, 277
- SEMPER, 233
- Serial Number, 73
- Server redundancy, 61
- Services of public-key cryptography, 12–17
 - core services, 37–48.
 - See also* Core PKI services
 - data integrity, 16
 - digital signature, 14–16
 - encryption, 14
 - key establishment, 16–17
 - other services, 17
 - PKI-enabled services, 49–67.
 - See also* PKI-enabled services
 - security between strangers, 12–14
- SET, 81–82, 180, 233
- SET certificate structure, 81
- SHA-1, 18–19
- SHA-2, 19
- Shamir, Adi, 17
- Shared repository, 168
- Short-lived certificates, 126
- SIA private extension, 78, 163
- Signatures, 73, 109
- Signing-on, 23
- Signing private key, 93

- Simple Authentication and Security Layer (SASI), 241
- Simple Certificate Validation Protocol (SCVP), 125, 255
- Simple Public-Key GSS-API Mechanism (SPKM), 240
- Simple Public Key Infrastructure (SPKI), 79–80, 228–229
- Simple substitution cipher, 9
- Single-factor authentication, 39
- Single sign-on (SSO), 24–25
- SIRCA proof of concept, 250
- SPKI, 79–80, 228–229
- SPKM, 240
- SSL/TLS, 290
- “Standard Specifications for Public Key Cryptography,” 230
- “Standard Specifications for Public Key Cryptography: Additional Techniques,” 230
- Standard vs. proprietary solutions, 274
- Standards, 219–258
 - ANSI X9F, 227
 - ECOM, 234
 - EDIFACT, 230
 - further reading, 253–258
 - GOC PKI, 232–233
 - ICE-CAR, 234–235
 - IEEE, 230
 - interoperability initiatives, 245–250
 - IPsec, 228, 239
 - ISO TC68, 226
 - JCP, 234
 - LDAP, 226, 238
 - MISPC, 232
 - ongoing work, 240–241
 - OpenPGP, 229–230
 - PFKI, 232
 - PKIX, 224–225, 238
 - role, 243–244
 - S/MIME, 227, 238–239
 - SEMPER, 233–234
 - SET, 233
 - SPKI, 228–229
 - TLS, 228, 239–240
 - toolkit requirements, 240
 - WAP, 230–231
 - web sites, 257
 - X.500, 225–226, 238
 - X.509, 223–224, 237
 - XML-based activities, 231
- Static-static DH, 46
- Status Referrals, 112
- Strategic decisions, 269–281. *See also*
 - Deployment considerations
- Strict hierarchy of CAs, 132–134
- Strict hierarchy of CAs trust model, 133
- Subject, 73
- Subject Alternative Name, 75
- Subject Directory Attributes, 76, 246
- Subject Information Access (SIA), 78, 163
- Subject key identifier, 74
- Subject Public Key Info, 73
- Subject Unique ID, 74
- Subordinate CAs, 132
- Subscriber responsibilities, 190–191
- Subsequent authentication, 39
- Suggested reading. *See* Further reading
- Symmetric central server architectures, 9
- Symmetric ciphers, 8–9
- TCO, 266
- TC68, 226
- This Update, 109
- Three-key pairs, 93
- TIE, 235
- Time Stamp Authority (TSA), 58
- Time stamping, 33, 50
- TLS, 167, 228, 239–240
- Toolkit-based session security, 240
- Total cost of ownership (TCO), 266
- “Towards a Practical Public-Key Cryptosystem” (Kohnfelder), 70
- Transport Layer Security (TLS), 167, 228, 239–240
- Trapdoor functions with high computational complexity, 11
- Trust, 131–132
- Trust anchor, 132, 146
- Trust Infrastructure for Europe (TIE), 235

- Trust models, 131–149
 - certificate path processing, 146–149
 - cross-certification, 143–145
 - distributed trust architecture, 135–138
 - entity naming, 145–146
 - four-corner model, 138–139
 - loose hierarchy of CAs, 134–135
 - policy-based hierarchies, 135
 - strict hierarchy of CAs, 132–134
 - user-centric trust, 142
 - web model, 139–141
- Trust networks, 292–293
- Trusted-issuer hierarchies, 134
- Trusted public key, 132
- Trusted time delivery mechanism, 61
- Trusted time sources, 58
- TSA, 58
- Two-key pair model, 93

- Unilateral cross-certification, 143
- U.S. Federal Bridge CA initiative, 168
- U.S. FPKI, 232
- User-centric trust, 142
- User key compromise, 176–178
- User Notice qualifier, 75

- Valicert, 120
- Validity, 73
- Vendor selection, 280
- Vendor's web sites, 296
- Verification certificate, 93
- VeriSign Trust Network (VTN), 293
- Veronyms, 56
- Version, 73, 109
- Version 1 public-key certificate, 71
- Version 2 CRLs, 108–110
- Version 2 public-key certificate, 71
- Version 3 certificate structure, 72

- Version 3 public-key certificate, 70, 71
- Vignette (real-life scenario), 203–206
- VTN, 293

- W3C, 231
- WAP Forum, 230
- WAP Security Group (WSG), 230, 231
- Web model, 139–141
- Web Services Security (WSS), 231
- Web sites. *See also* Further reading
 - standards bodies, 257
 - vendors, 296
- Wireless Application Protocol Forum (WAP Forum), 230
- World Wide Web Consortium (W3C), 231
- WPKI, 230
- WSG, 230, 231
- WSS, 231
- WTLS, 230

- X9F, 227
- X9F1, 227
- X9F3, 227
- X9F5, 227
- X.500, 225–226, 238
- X.509, 223–224, 237
- X.509 public-key certificate, 70
- X.509 recommendation certificate/
CRL profile, 246
- XACML, 59, 231
- XKMS, 223, 231, 241, 256
- XML-based activities, 231
- XML Encryption, 231
- XML Key Management Specification, 231
- XML Signature, 231

- Zero-knowledge, 17
- Zimmermann, Phil, 80