

# Index

## Symbols

**\$/** shortcut for **\$(file.separator)** 284  
**\$(property)** to specify property value 283–285  
**/** always used in codeBase URLs as directory separator 278  
**/** at end of codeBase URL 278  
**/-** at end of codeBase URL 278  
**/\*** at end of codeBase URL 278  
**\\** for single backslash in file paths 281

## A

**Abstract Syntax Notation 1 (ASN.1) standard** 131, 194  
**accept method** 251  
**acceptSecContext method** 244, 248  
**access control**  
     algorithm  
         basic 94–97  
         extended 98–101  
         full 107–109, 150–152  
     code-centric 142  
     context  
         *See* context  
     principal-based 150–152  
     user-centric 142  
**AccessControlContext class** 90–91, 94, 105–109, 124–125, 150–151  
     *See also* context  
**AccessControlException class** 94, 158  
**AccessController class** 92–112, 150–151  
     interface design 93  
     versus **SecurityManager class** 109–110  
**actions, permissions** 60

## add method

**PermissionCollection class** 66  
     **Permissions class** 67  
**adding providers** 187, 273–274  
**addProvider method** 187, 273  
**AES (Advanced Encryption Standard)** 14, 233, 236  
**algorithm specifications** 237–240  
**algorithm-independent initialization** 202  
**AlgorithmParameterGenerator class** 194  
**AlgorithmParameters class** 193, 213  
**AlgorithmParameterSpec interface** 193  
**algorithm-specific initialization** 203  
**alias, keystore entry** 205, 290  
**aliases method** 205  
**AllPermission class** 63–64, 68  
**AppletClassLoader class** 44, 49, 53  
**applets** 25  
     signed 29–30  
**appletviewer utility program** 44–45, 271  
**application class loader** 43, 45, 49  
**application class path** 55–56  
**application classes** 43  
**architecture, security**  
     benefits 37  
     customizing 113–125  
     deploying 265–308  
     new, reasons for 31–34  
     original 25–27  
     overview 34–39  
**ASN.1 (Abstract Syntax Notation 1) standard** 131, 194  
**asymmetric cipher** 15–16  
**AudioPermission class** 62

**auditing permission calls** 119–120

**authenticated identity** 127

**authentication**

digital signature 138

distributed end entity 152–156

entity 127

JAAS 141–148, 153

Java GSS-API 152–154, 242

JSSE 152, 155–156

overview 16–19

peer-to-peer 152

**Authenticator class** 152–153

**authorization** 141–142, 149–152

**AuthPermission class** 62

**AWTPPermission class** 62, 114

## B

**Base64 encoding** 131, 140, 225

**BasicPermission class** 59–60, 62–63

**Bell-LaPadula confidentiality model** 8, 12

**Blowfish**

algorithm description 231

standard algorithm name 231, 233, 236

SunJCE implementation 186, 209, 214

**bootstrap class loader** 38, 42, 45

**Bracha, G.** 43

**build method** 136

**bytecode verification** 26–29

## C

**CA**

*See* Certification Authority

**cacerts keystore file** 295–296

**CallbackHandler interface** 147–149

**callbacks, for login modules** 148–149

**Cambridge Time-Sharing Computer System** 13

**CBC (Cipher Block Chaining mode)** 234

**certificate chains** 16, 293, 295

**Certificate class** 134, 144

programming example 225–226

**certificate reply** 225, 293–294

**Certificate Revocation List (CRL)** 130, 134, 201

**Certificate Signing Request (CSR)** 132, 225

keytool generation of 293, 298, 300

**certificate type standard names** 232

**CertificateFactory class** 134–135, 201

programming example 225–226

**certificates**

*See* digital certificates

**Certification Authority** 128, 132, 225

**certification path** 128, 134–137

**Certification Practice Statement (CPS)** 132

**CertPath class** 135–136

**CertPathBuilder class** 136–137

**CertPathBuilderException class** 136

**CertPathBuilderResult interface** 136

**CertPathParameters interface** 136

**CertPathValidator class** 135, 137

**CertPathValidatorResult interface** 135

**CertStore class** 137

**CFB (Cipher Feedback mode)** 234

**checkGuard method** 172, 174–175

**checkPermission method**

AccessControlContext class 90

AccessController class 90–91, 93–94, 109–110, 125

SecurityManager class 88–90, 92–93, 109–110

**Chinese Remainder Theorem (CRT)** 198–199

**Chinese Wall security model** 11

**cipher**

*See also* Cipher class

asymmetric 15–16

definition 178

standard names for algorithm, mode, and

padding 233

symmetric 14

**Cipher Block Chaining mode (CBC)** 234

**Cipher class** 208–214

*See also* cipher

programming example 226–227

**Cipher Feedback mode (CFB)** 234

**ciphertext** 14–15

**Clark-Wilson integrity model** 11

**class loading** 41–56

application class loader 43, 45, 49

bootstrap class loader 38, 42, 45

custom class loaders 44

defining a class 50–51

defining class loader 42, 46

delegation of class loader 45–50

extension class loader 43, 45

initiating class loader 42, 45

*Index*

- lazy loading 41
- multiple namespaces 41
- primordial class loader 38, 42
- classes (concepts and use)**
  - association with ProtectionDomains 74
  - class type 42
  - defining 50–51
  - file format 25, 42
  - files 42
  - finding 47
  - inner classes, security issues 167
  - loading
    - See* class loading
  - paths 55–56
  - system classes 43, 55–56, 78
- classes (listed by name)**
  - AccessControlContext 90–91, 94, 105–109, 124–125, 150–151
  - AccessControlException 94, 158
  - AccessController 92–112, 150–151
  - AlgorithmParameterGenerator 194
  - AlgorithmParameters 193, 213
  - AllPermission 63–64, 68
  - AppletClassLoader 44, 49, 53
  - AudioPermission 62
  - Authenticator 152–153
  - AuthPermission 62
  - AWTPermission 62, 114
  - BasicPermission 59–60, 62–63
  - Certificate 134, 144, 225–226
  - CertificateFactory 134–135, 201, 225–226
  - CertPath 135–136
  - CertPathBuilder 136–137
  - CertPathBuilderException 136
  - CertPathValidator 135, 137
  - CertStore 137
  - Cipher 208–214, 226–227
  - ClassLoader 43, 45
  - CodeSource 69–74
  - Configuration 146
  - CRL 134
  - DelegationPermission 62, 245, 247
  - DESedeKeySpec 216
  - DESKeySpec 216–217
  - DSAPrimitiveKeySpec 193, 222
  - DSAPrivateKeySpec 197–198, 223
  - DSAPublicKeySpec 198, 200, 224
  - EncodedKeySpec 199
  - FileInputStream 175–176
  - FilePermission 58–60, 119, 175
  - GSSManager 242–245, 247
  - GuardedObject 172–176
  - HttpsURLConnection 253–254
  - InvalidAlgorithmParameterException 136, 210
  - InvalidKeyException 210
  - IvParameterSpec 214
  - KeyAgreement 217–219
  - KeyFactory 185, 200, 223–224
  - KeyFactorySpi 185
  - KeyGenerator 215–216, 226
  - KeyManagerFactory 250, 258–260
  - KeyPair 202, 222–224
  - KeyPairGenerator 202, 222
  - KeyStore 137, 203–205, 257, 291–292
  - Krb5LoginModule 152, 154–155
  - Logger 119
  - LoggingPermission 62
  - LoginContext 146–147
  - Mac 219–220
  - MessageDigest 185, 188–189, 220–222
  - MessageDigestSpi 185
  - MessageProp 249
  - NetPermission 62
  - PasswordAuthentication 153
  - PBEKeySpec 216, 227, 230
  - PBEParameterSpec 214, 229
  - Permission 59–62, 113, 174
  - PermissionCollection 66–67, 114
  - Permissions 67
  - PKCS8EncodedKeySpec 199
  - PKIXParameters 136
  - Policy 57, 80–82
  - PrivateCredentialPermission 145
  - PropertyPermission 62, 114
  - ProtectionDomain 50–51, 74–79, 152
  - Provider 188, 273
  - Random 206
  - ReflectPermission 62, 68
  - RSAMultiPrimePrivateCrtKeySpec 199
  - RSAPrivateCrtKeySpec 198
  - RSAPrivateKeySpec 198–199
  - RSAPublicKeySpec 199
  - RuntimePermission 60, 62, 113–114
  - SealedObject 171–172
  - SecretKeyFactory 216–217, 229

**classes (listed by name), continued**

SecretKeySpec 217  
 SecureClassLoader 43–53  
 SecureRandom 206–208, 222  
 Security 187–188  
 SecurityException 82, 158  
 SecurityManager 87–90, 92, 109–110, 118–120, 150  
 SecurityPermission 62  
 SerializablePermission 62  
 ServerSocketFactory 250  
 ServicePermission 154–155, 245–247  
 Signature 169, 184, 190–192, 222–224  
 SignatureSpi 184  
 SignedObject 168–171  
 SocketFactory 250  
 SocketPermission 113  
 SQLPermission 62  
 SSLContext 250, 252, 254–256  
 SSLPermission 62  
 SSLServerSocket 250–251  
 SSLServerSocketFactory 250–252  
 SSLSocket 250–252  
 SSLSocketFactory 250–253, 255  
 Subject 144–152, 154  
 SubjectDomainCombiner 125  
 System 89  
 TrustAnchor 136  
 TrustManagerFactory 250, 256–258  
 UnresolvedPermission 64–66  
 URLClassLoader 43–44, 49, 53–54  
 X500Principal 283, 306  
 X509Certificate 134, 201  
 X509CRL 134, 201  
 X509CRLEntry 134  
 X509EncodedKeySpec 200, 224  
**ClassLoader class** 43, 45  
**CLASSPATH** 43, 55–56  
**client containers** 324–325  
**clone method** 165  
**codeBase** 277–278  
**code-centric access control** 142  
**CodeSource class** 69–74  
**combine method** 91, 125  
**Comité Consultatif International Téléphonique et Télégraphique** 128

**confidentiality**

of data 3, 12, 248  
 of objects 157, 171

**Configuration class** 146**context**

access control 90–91, 94, 105–109, 124  
*See also* AccessControlContext class  
 GSS-API  
*See* GSSContext interface

**covert channels** 9–10**CPS (Certification Practice Statement)** 132**createAccessControlContext permission** 92**createClassLoader permission** 46**createContext method** 244**createCredential method** 243**createName method** 242–243**createSecurityManager permission** 88**credentials**

cache 154  
 delegation 244, 248  
 Java GSS-API 242–246  
 overview 144–145  
 types 155

**CRL (Certificate Revocation List)** 130, 134, 201**CRL class** 134**cryptanalysis** 12**Cryptographic Service Provider (CSP)**

*See* providers

**cryptography** 12–16

*See also* JCA; JCE

concepts 178–179

services 179, 182

versus computer security 2, 12

**cryptology** 12**CSP (Cryptographic Service Provider)**

*See* providers

**CSR (Certificate Signing Request)** 132, 225

keytool generation of 293, 298, 300

**customizing the security architecture** 113–125**D****DAC (discretionary access control) security model** 8**Damgård, I. B.** 13

*Index***Data Encryption Standard***See* DES**decidability of system security** 11**decryption**

definition 178

keys used for 15

of data 210–211

of SealedObject 171

of signature 139

programming example 226–227

reversibility 16

**defineClass method**

ClassLoader class 50–51

SecureClassLoader class 52

**delegation**

class loader 45–50

credentials, Java GSS-API 247

**DelegationPermission class** 62, 245, 247**deleteEntry method** 205**denial-of-service attacks** 3**deploying the security architecture** 265–308**DER (Distinguished Encoding Rules) standard** 131, 197**DES (Data Encryption Standard)**

algorithm description 14, 231

programming example 226

standard algorithm name 231, 234, 236

SunJCE implementation 186, 209, 214

**DES-EDE (triple DES) cipher algorithm**

SunJCE implementation 209, 214

**DESede standard algorithm name** 231, 234, 236**DESedeKeySpec class** 216**deserialization** 163**DESKeySpec class** 216–217**Diffie-Hellman**

algorithm description 16, 231

keys 216, 218

**DiffieHellman standard algorithm name** 231**digest***See* hash**digest method** 189, 221**digital certificates***See also* Certificate Revocation List; certification path; X.509, certificates

APIs 133

Base64 encoding 131

chains 16, 128

fingerprints 294, 299

generating 201

issuer 131

obtaining 131

overview 128–134

public key 128–137

reading file containing 225–226

referenced by CodeSource 69

root certificate 16, 128

self-signed 16, 131

subject 131–132

**digital signature**

ciphertext used as 16

of code 29, 138–141

description 178

generating and verifying 222–224

**Digital Signature Algorithm***See* DSA**digital signature algorithm standard names** 231**dispose method** 248**Distinguished Encoding Rules (DER) standard** 131, 197**Distinguished Name (DN)** 129, 131, 300

sample 306–307

**distributed end-entity authentication** 152–156**DN (Distinguished Name)** 129, 131, 300

sample 306–307

**DNS (Domain Name Service)** 19**doAs**

method 150–151

*See also* privileged code

permission 151

**doAsPrivileged**

method 150–151

*See also* privileged code

permission 151

**doFinal method**

Cipher class 210–211, 213–214, 227, 230

Mac class 220

**Domain Name Service (DNS)** 19**DomainCombiner interface** 91–92, 124–125, 152**domains***See* protection domains

**doPhase method** 218  
**doPrivileged method** 91, 93, 99–109, 125, 162  
*See also* privileged code  
**DSA (Digital Signature Algorithm)**  
 description 231  
 KeyFactory 182  
 key-pair generation algorithm specification 239–240  
 limitations 16  
 parameter generation algorithm specification 240  
 programming examples 222–224  
 signature algorithm specification 238  
 standard algorithm name 231  
**DSAParameterSpec class** 193, 222  
**DSAPrivateKeySpec class** 197–198, 223  
**DSAPublicKeySpec class** 198, 200, 224  
 programming example 224  
**dynamic policy** 84

## E

**eager evaluation implementation** 108  
**ECB (Electronic Code Book mode)** 209, 226, 234  
**Electronic Code Book mode (ECB)**  
*See* ECB  
**EMACS** 20  
**EncodedKeySpec class** 199  
**encryption**  
 definition 178  
 keys used for 15  
 of data 210–211  
 of digest (hash) 139  
 of SealedObject 171  
 programming example 226–230  
 reversibility 16  
**end entity** 132  
**engine classes** 179, 182–185  
**equals method**  
 AllPermission class 63  
 BasicPermission class 63  
 CodeSource class 70–71  
 Permission class 60  
**extension class loader** 43, 45

## F

**factory** 184

**FileInputStream class** 175–176  
**FilePermission class** 58–60, 119, 175  
**findClass method**  
 ClassLoader class 47  
 URLClassLoader class 53  
**findLoadedClass method** 47–48  
**fingerprints (file hash values)** 65, 178, 294, 299  
**firewalls** 6–7

## G

**generateCertificate method** 201, 225  
**generateCertificates method** 201, 225  
**generateCertPath method** 135  
**generateCRL method** 201  
**generateCRLs method** 201  
**generateKey method** 172, 216, 226  
**generateKeyPair method** 203, 222  
**generateParameters method** 196  
**generatePrivate method** 200, 223  
**generatePublic method** 200, 224  
**generateSecret method** 217, 219, 229  
**generateSeed method** 208  
**generator** 184  
**Generic Security Service API**  
*See* GSS-API  
**getAlgorithm method** 196, 212  
**getCertificate method** 205  
**getCertificateAlias method** 205  
**getCertificateChain method** 205  
**getCertPath method** 136  
**getClassContext method** 88  
**getClassLoader**  
 method 46–47  
 permission 47  
**getContext method** 91, 94, 125  
**getDefault method**  
 SSLServerSocketFactory class 250  
 SSLSocketFactory class 250, 252, 255  
**getDefaultType method** 204, 292, 302  
**getDelegCred method** 244  
**getEncoded method** 194, 197, 213, 224  
**getFormat method** 197  
**getInstance method**  
 AlgorithmParameterGenerator class 195  
 AlgorithmParameters class 193, 213  
 Certificate class 201  
 CertificateFactory class 134–135, 201, 225

## Index

345

- CertPathBuilder class 136
  - CertPathValidator class 136–137
  - Cipher class 172, 208–209, 213, 227, 230
  - GSSManager class 242
  - KeyAgreement class 217
  - KeyFactory class 200, 223
  - KeyGenerator class 172, 215, 226
  - KeyManagerFactory class 259
  - KeyPairGenerator class 202, 222
  - KeyStore class 204
  - Mac class 219
  - MessageDigest class 188, 221
  - SecretKeyFactory class 216–217, 229
  - SecureRandom class 207, 222
  - Signature class 169, 190, 222–224
  - SSLContext class 250, 255
  - TrustManagerFactory class 256–257
  - getKey method** 205
  - getKeyManagers method** 250
  - getKeySpec method** 201, 224
  - getMIC method** 248–249
  - getObject method** 170
  - getOutputSize method** 214
  - getParameters method** 213
  - getParameterSpec method** 192, 194
  - getParent method** 45–47
  - getPasswordAuthentication method** 153
  - getPermissions method**
    - Policy class 81–82
    - SecureClassLoader class 52–53
    - URLClassLoader class 53
  - getPolicy**
    - method 81–82
    - permission 81
  - getPrivate method** 223
  - getProperty method** 188, 302
  - getProtectionDomain**
    - method 51, 78, 88
    - permission 51, 78
  - getProvider method** 187
  - getProviders method** 187
  - getPublic method** 223
  - getSecurityContext method** 89–90
  - getSecurityManager method** 89
  - getSubject permission** 245
  - getSubjectFromDomainCombiner permission** 245
  - getSupportedProtocols method** 255
  - getSystemClassLoader method** 43, 45–47, 49
  - getTrustManagers method** 250
  - Goguen, J. A.** 10
  - grant entries in policy files** 276–281
  - GSS-API (Generic Security Service API)**
    - 143, 154
    - See also* Java GSS-API
  - GSSContext interface** 242, 247–249
  - GSSCredential interface** 242–246
  - GSSManager class** 242–245, 247
  - GSSName interface** 242–243
  - Guard interface** 172–176
  - GuardedObject class** 172–176
- ## H
- hash** 13–14, 138–139, 179, 220–222
    - definition 178
  - High-Watermark security model** 11
  - HMAC definition** 179
  - HmacMD5 standard algorithm name** 236
  - HMAC-MD5 SunJCE implementation** 220
  - HmacSHA1 standard algorithm name** 236–237
  - HMAC-SHA1 SunJCE implementation** 220
  - HostnameVerifier interface** 253
  - HttpsURLConnection class** 253–254
- ## I
- IETF (Internet Engineering Task Force)** 17
  - immutability**
    - of CodeSource objects 70
    - of objects 161–162
    - of Permission objects 61
  - implies method**
    - AllPermission class 63
    - BasicPermission class 63, 114
    - CodeSource class 70–73
    - Permission class 60–61
    - PermissionCollection class 66
    - Permissions class 67
    - Policy class 81
    - ProtectionDomain class 77
  - inheritance**
    - context 105
    - method 97–98

**init method**

AlgorithmParameterGenerator class 195  
 AlgorithmParameters class 193, 213  
 Cipher class 172, 209, 213–214, 227, 230  
 KeyAgreement class 218  
 KeyGenerator class 215  
 KeyManagerFactory class 250, 259  
 Mac class 219  
 SSLContext class 250, 254–255  
 TrustManagerFactory class 250, 257

**initialize method** 202–203, 222**initiating class loader** 42, 45**initSecContext method** 244, 248**initSign method** 190, 223**initVerify method** 190, 223–224**inner classes, security issues** 167**insertProvider.providerName permission** 273**insertProviderAt method** 187, 273**installation directory <java.home>** 266–267**installing**

J2SE 266  
 providers 271–272  
 security manager 89, 271

**integrity**

of data 3–4, 11–13, 138  
 of objects 157, 171  
 protection 248

**interfaces (listed by name)**

AlgorithmParameterSpec 193  
 CallbackHandler 147–149  
 CertPathBuilderResult 136  
 CertPathParameters 136  
 CertPathValidatorResult 135  
 DomainCombiner 91–92, 124–125, 152  
 GSSContext 242, 247–249  
 GSSCredential 242–246  
 GSSName 242–243  
 Guard 172–176  
 HostnameVerifier 253  
 Key 196–197  
 KeyManager 155, 250, 256, 258  
 KeySpec 197–198  
 LoginModule 146  
 ManagerFactoryParameters 257  
 Principal 74, 144, 149–152, 154  
 PrivateKey 197

PrivilegedAction 100, 102–107

PrivilegedExceptionAction 104–105, 151

PublicKey 197

SecretKey 217, 219

Serializable 163–168, 171

SSLSession 250, 252

TrustManager 250, 256

X509Extension 134

**International Telecommunication Union (ITU)** 128**Internet Engineering Task Force (IETF)** 17**InvalidAlgorithmParameterException class** 136, 210**InvalidKeyException class** 210**IPSec protocol** 133, 142**isCertificateEntry method** 205**isKeyEntry method** 205**isProtReady method** 248**ITU (International Telecommunication Union)** 128**IvParameterSpec class** 214**J****J2EE** 323–324**JAAS (Java Authentication and Authorization Service)** 141–152

authentication 141–148, 153  
 authorization 149–152  
 callbacks 148  
 credentials 144  
 login configuration files 286–289  
 principal-based access control 150–152  
 principals 143  
 subjects 143

**JAR files**

description 301  
 example of signing and verification 304–306  
 format 139–141  
 signature verification 299, 303–304  
 signing 301–303

**jar tool** 301**jarsigner utility** 203, 301–306

example of JAR file signature and verification 304–306  
 file extensions 302  
 JAR file signature verification 303–304

*Index*

JAR file signing 301–303

options

- keypass 301, 304
- keystore 301, 304
- sigFile 302
- signedjar 301, 304
- storepass 301, 304
- storetype 291, 301
- verbose 305

**Java**

- application 25
- platform 20, 25
- programming language 24–26
- technology 20
- virtual machine

*See* JVM

**Java 2 Micro Edition** 314–316

**Java Authentication and Authorization Service (JAAS)**

*See* JAAS

**Java Card** 310–314

**Java Certification Path API**

- basic classes 135
- building classes 136
- certificate/CRL storage classes 137
- overview 133–137
- PKIX classes 137
- validation classes 135–136

**Java Cryptography Architecture**

*See* JCA

**Java Cryptography Extension**

*See* JCE

**Java Generic Security Service API**

*See* Java GSS-API

**Java GSS-API (Java Generic Security Service API)**

- authentication 152–154, 242
- confidentiality and integrity controls 242–249
- credential delegation 247
- message security 249
- security context establishment 247–249

**Java Plug-in** 45

**Java Remote Method Invocation (Java RMI)** 157

**Java Secure Socket Extension**

*See* JSSE

**Java Web Start** 45

**java.home system property** 266

**java.security security properties file** 268–269

**java.security.manager system property** 271

**java.security.policy system property** 121, 271

**java.security.properties system property** 270

**JCA (Java Cryptography Architecture)** 177–240

*See also* cryptography; JCE

algorithm parameters 192–196

concepts 178–179

core classes 187–208

design principles 179–180

JCE classes 208–220

**JCE (Java Cryptography Extension)** 177, 181–240

*See also* cryptography; JCA

classes 208–220

**JCEKS keystore type** 204, 233

**JDK to Java 2 SDK terminology shift** 30

**Jini Network Technology** 320–323

**JKS keystore type** 155, 204, 233, 291, 296

**JSSE (Java Secure Socket Extension)**

authentication 152, 155–156

confidentiality and integrity controls 249–260

core classes 250–260

SSL context establishment 250

**JVM (Java virtual machine)** 21, 24–29, 41, 45

**K****Kerberos**

*See also* Krb5LoginModule class

mechanism 143

protocol 17, 142

tickets 144

V5 GSS-API mechanism 153–154, 242–249

**key agreement** 178

**key algorithm standard names** 231

**key distribution centers** 17

**key entry** 155, 289

**key generator algorithm standard names** 236

**Key interface** 196–197

**key manager** 254, 256, 258

*See also* KeyManager interface

**key-pair generation**

*See* KeyPairGenerator class; keytool utility

**key specification** 223**KeyAgreement class** 217–219**KeyFactory class** 185, 200

programming example 223–224

**KeyFactorySpi class** 185**KeyGenerator class** 215–216, 226**KeyManager interface** 155, 250, 256, 258**KeyManagerFactory class** 250, 258–260**KeyNote** 144**KeyPair class** 202, 222–224**KeyPairGenerator class** 202

programming example 222

**keys**

cryptographic 144

encryption 4, 12

private 15, 128, 132, 139

public 15–16, 128, 132–134, 139

secret 12, 14, 16–17, 178, 216, 219

unwrapping 211–212

wrapping 211–212

**KeySpec interface** 197–198**keystore**

*See also* Keystore class

cacerts file 295–296

default file name 291

default implementation 289

definition 155

description and use 289–292

policy file entry 276

standard names for types 233

type 291, 296, 301

**KeyStore class** 137, 203–205, 257, 291–292

*See also* keystore

**keystore.type security property** 291–292, 302**keytool utility** 131, 203, 292–300

cacerts keystore file 295–296

Certificate Signing Request (CSR) generation 293, 298, 300

certificates

exporting 296, 299

importing 294–296, 299

importing certificate reply 295, 299–300

printing information for 294, 299

**commands**

-certreq 293, 298, 300

-delete 300

-export 296, 299

-genkey 290, 293, 297

-help 297

-import 294–296, 299–300

-keyclone 300

-keypasswd 291

-list 296

-printcert 294, 299

-selfcert 300

**defaults** 292**examples of use** 297–300**help** 297**key-pair generation** 290, 293, 297**keystore creation** 297**keystore entry**

aliases 290

cloning 300

removing 300

**options**

-alias 290

default values 297

-dname 306

-keystore 291

ordering 292

-rfc 296

-storepass 297

-storetype 291

-trustcacerts 295–296

**password**

assigning 297

changing 291

**printing keystore contents** 296**self-signed certificate generation** 300**Knuth, Donald** 13**Krb5LoginModule class** 152, 154–155

*See also* Kerberos

**L****Lampson, B. W.** 9**lazy evaluation implementation** 108**lazy loading** 41**LDAP (Lightweight Directory Access Protocol)** 133, 137

*Index***least privilege, principle of** 97, 138**legacy systems** 11**Liang, S.** 43**Lightweight Directory Access Protocol (LDAP)** 133, 137**linking** 41**LISP** 20**load method** 204**loadClass methods** 47–49**loading classes***See* class loading**Logger class** 119**logging permission calls** 119–120**LoggingPermission class** 62**login configuration files** 286–289**login context** 145–149**login module** 146–149, 286–288**LoginContext class** 146–147**LoginModule interface** 146**M****MAC (mandatory access control) security model** 8–10**MAC (message authentication code)** 13, 178, 219–220**Mac algorithm standard names** 236**Mac class** 219–220**ManagerFactoryParameters interface** 257**manifest file** 139–140**MD2 message digest algorithm** 238**MD2withRSA signature algorithm** 238**MD5 message digest algorithm**

specification 238

use in HMAC 179

**MD5withRSA signature algorithm** 238**Merkle, R. C.** 13**Meseguer, J.** 10**message authentication code (MAC)** 13, 178, 219–220**message digest (hash)**

algorithm standard names 230

definition 178

example of computing 220–222

**MessageDigest class** 185, 188–189

programming example 220–222

**MessageDigestSpi class** 185**MessageProp class** 249**META-INF JAR file directory** 139**methods (listed by name)**

accept 251

acceptSecContext 244, 248

add

PermissionCollection class 66

Permissions class 67

addProvider 187, 273

aliases 205

build 136

checkGuard 172, 174–175

checkPermission

AccessControlContext 90

AccessControlContext class 90

AccessController class 90–91, 93–94, 109–110, 125

SecurityManager class 88–90, 92–93, 109–110

clone 165

combine 91, 125

createContext 244

createCredential 243

createName 242–243

defineClass

ClassLoader class 50–51

SecureClassLoader class 52

deleteEntry 205

digest 189, 221

dispose 248

doAs 150–151

doAsPrivileged 150–151

doFinal

Cipher class 210–211, 213–214, 227, 230

Mac class 220

doPhase 218

doPrivileged 91, 93, 99–109, 125, 162

equals

AllPermission class 63

BasicPermission class 63

CodeSource class 70–71

Permission class 60

findClass

ClassLoader class 47

URLClassLoader class 53

findLoadedClass 47–48

generateCertificate 201, 225

generateCertificates 201, 225

generateCertPath 135

generateCRL 201

**methods (listed by name), continued**

- generateCRLs 201
- generateKey 172, 216, 226
- generateKeyPair 203, 222
- generateParameters 196
- generatePrivate 200, 223
- generatePublic 200, 224
- generateSecret 217, 219, 229
- generateSeed 208
- getAlgorithm 196, 212
- getCertificate 205
- getCertificateAlias 205
- getCertificateChain 205
- getCertPath 136
- getClassContext 88
- getClassLoader 46–47
- getContext 91, 94, 125
- getDefault
  - SSLServerSocketFactory class 250
  - SSLSocketFactory class 250, 252, 255
- getDefaultType 204, 292, 302
- getDelegCred 244
- getEncoded 194, 197, 213, 224
- getFormat 197
- getInstance
  - AlgorithmParameterGenerator class 195
  - AlgorithmParameters class 193, 213
  - Certificate class 201
  - CertificateFactory class 134–135, 201, 225
  - CertPathBuilder class 136
  - CertPathValidator class 136–137
  - Cipher class 172, 208–209, 213, 227, 230
  - GSSManager class 242
  - KeyAgreement class 217
  - KeyFactory class 200, 223
  - KeyGenerator class 172, 215, 226
  - KeyManagerFactory class 259
  - KeyPairGenerator class 202, 222
  - KeyStore class 204
  - Mac class 219
  - MessageDigest class 188, 221
  - SecretKeyFactory class 216–217, 229
  - SecureRandom class 207, 222
  - Signature class 169, 190, 222–224
  - SSLContext class 250, 255
  - TrustManagerFactory class 256–257
- getKey 205
- getKeyManagers 250
- getKeySpec 201, 224
- getMIC 248–249
- getObject 170
- getOutputSize 214
- getParameters 213
- getParameterSpec 192, 194
- getParent 45–47
- getPasswordAuthentication 153
- getPermissions
  - Policy class 81–82
  - SecureClassLoader class 52–53
  - URLClassLoader class 53
- getPolicy 81–82
- getPrivate 223
- getProperty 188, 302
- getProtectionDomain 51, 78, 88
- getProvider 187
- getProviders 187
- getPublic 223
- getSecurityContext 89–90
- getSecurityManager 89
- getSupportedProtocols 255
- getSystemClassLoader 45–47, 49
- getTrustManagers 250
- implies
  - AllPermission class 63
  - BasicPermission class 63, 114
  - CodeSource class 70–73
  - Permission class 60–61
  - PermissionCollection class 66
  - Permissions class 67
  - Policy class 81
  - ProtectionDomain class 77
- init 195
  - AlgorithmParameters class 193, 213
  - Cipher class 172, 209, 213–214, 227, 230
  - KeyAgreement class 218
  - KeyGenerator class 215
  - KeyManagerFactory class 250, 259
  - Mac class 219
  - SSLContext class 250, 254–255
  - TrustManagerFactory class 250, 257
- initialize 202–203, 222
- initSecContext 244, 248
- initSign 190, 223
- initVerify 190, 223–224
- insertProviderAt 187, 273
- isCertificateEntry 205
- isKeyEntry 205

*Index*

351

- isProtReady 248
- load 204
- loadClass 47–49
- newInstance 54
- newPermissionCollection 60–61, 66
- nextBytes 207
- Oid 242
- readObject 163–167
- readPasswd 228
- readResolve 165
- refresh 81–82
- removeProvider 187
- requestCredDeleg 244
- requestPasswordAuthentication 153
- resolveClass 47, 49
- run
  - PrivilegedAction interface 100–105, 107, 151
  - PrivilegedExceptionAction interface 151
- setCertificateEntry 205
- setDefaultSSLSocketFactory 253
- setEnabledProtocols 255
- setKeyEntry 205
- setPolicy 81–82
- setProperty
  - Security class 188
  - System class 267
- setSecurityManager 89
- setSeed 207, 222
- setSigners 51
- setSSLSocketFactory 253
- sign 191, 223
- store 205
- toString 60–61
- unwrap 212, 249
- update
  - Cipher class 211, 214
  - Mac class 220
  - MessageDigest class 189, 221
  - Signature class 191, 223–224
- validate 136
- verify 170, 191, 223–224
- verifyMIC 249
- wrap 211, 248–249
- writeObject 164
- Meyer, C. H.** 13
- Microsoft Windows** 21
- Microsoft Word documents with macros** 19
- MIT (Massachusetts Institute of Technology)** 17
- mobile code** 19–20
- modes**
  - Cipher initialization 209–212
  - Cipher transformation 208, 234
- mutability of objects** 161–162
- mutual authentication** 248
- N**
- names**
  - permission target names 60
  - standard 230–237
- namespaces, multiple** 41
- Naor, M.** 13
- native methods, security issues** 167
- Needham, Roger** 13
- Needham-Schroeder protocol** 17–18
- NetPermission class** 62
- network security** 241–263
- newInstance method** 54
- newPermissionCollection method** 60–61, 66
- nextBytes method** 207
- NONE cipher mode** 234
- NoPadding** 235
- O**
- OAEPWith<digest>And<mgf>Padding** 235
- object**
  - guarding
    - See GuardedObject class
  - identifier (OID) 154
  - sealing
    - See SealedObject class
  - security 157–176
  - signing
    - See SignedObject class
- OFB (Output Feedback mode)** 234
- OID (object identifier)** 154
- Oid method** 242
- one-time pad** 12
- one-way hash** 13–14, 138–139, 179, 220–222
  - definition 178
- opaque key representation** 196, 200, 216
- opaque parameter representation** 192
- OTP standard** 17
- Output Feedback mode (OFB)** 234
- overt channels** 9

**P****padding schemes, cipher** 208, 235**PAM** 145**parameter algorithm standard names** 231**PasswordAuthentication class** 153**password-based encryption***See* PBE**passwords, problems with** 19**PBE (password-based encryption)**

algorithm description 178

programming example 212, 227–230

standard algorithm name 231

**PBEKeySpec class** 216

programming example 227, 230

**PBEParameterSpec class** 214

programming example 229

**PBEWith<digest>And<encryption>** 234, 236**PBEWith<mac>** 237**PBEWith<prf>And<encryption>** 234, 236**PBEWithHmacSHA1AndDESede** 234**PBEWithMD5AndDES** 214, 234**PCBC (Propagating Cipher Block Chaining)** 234**PEM (Privacy Enhancement for Internet Electronic Mail)** 129**perimeter defense** 4–8**Permission class** 59–62, 113, 174**permission classes***See* classes (listed by name) for Permission class names**permission policy file entry** 279–281**PermissionCollection class** 66–67, 114**permissions (concepts and use)**

actions argument 60

assigning 83–84

checking 88, 94–101, 107–109

creating new types 113–118

dangers of granting 67–68

equality 61

equivalence 61

implication 61

*See also* implies method

named permissions 62

names 60

positive versus negative 59, 68–69

sets 66–67

spanning 86, 124

target name argument 60

unresolved 64–66

**Permissions class** 67**PGP certificates** 134**PKCS #1** 235**PKCS #5–style padding** 226**PKCS #7** 225, 294**PKCS #8** 197, 200**PKCS12 keystore type** 155, 233**PKCS5Padding** 209, 235**PKCS8EncodedKeySpec class** 199**PKIX**

algorithm 135–136

classes 137

standards 132

**PKIXParameters class** 136**plaintext** 14–15**pluggable authentication** 145**policy***See also* Policy class

appending 270–271

customizing 118–124

definition 57

enforcing 87–112

files, examples 281–283

format, default 276–281

locations 274–276

management for nonexperts 307–308

overriding 270–271

overview 79–82

specifying 57–84

store (repository) 120

**Policy class** 57, 80–82*See also* policy

alternative implementation 285–286

default implementation 80

**Policy provider, custom** 120–124**Policy Tool** 203**policy.allowSystemProperty security property** 121, 271**policy.provider security property** 285**policy.url.n security properties** 121, 275**PostScript files** 19**preference order** 181, 273**primordial class loader** 38, 42**principal** 143–144**Principal interface** 74, 144, 149–152, 154**principal policy file entry** 277–279

*Index*

**principal-based access control** 150–152  
**principle of least privilege** 97, 138  
**Privacy Enhancement for Internet Electronic Mail (PEM)** 129  
**private key** 15  
**PrivateCredentialPermission class** 145  
**PrivateKey interface** 197  
**privileged code**  
     *See also* doAs method; doAsPrivileged method; doPrivileged method  
     brief history 110–112  
     overview 98–109  
     security issues 162–163  
**PrivilegedAction interface** 100, 102–107  
**PrivilegedExceptionAction interface** 104–105, 151  
**PRNG (pseudo-random-number generator)** 206–207  
**Propagating Cipher Block Chaining (PCBC)** 234  
**properties**  
     expansion in policy files 283–285  
     security  
         appending 270  
         default values 269  
         keystore.type 291–292, 302  
         overriding 270  
         policy.allowSystemProperty 121, 271  
         policy.provider 285  
         policy.url.*n* 121, 275  
         security.overridePropertiesFile 270  
         security.provider.*n* 273  
         setting values for 268–269  
     system  
         java.home 266  
         java.security.manager 271  
         java.security.policy 121, 271  
         java.security.properties 270  
         setting values for 267  
         user.home 268  
**PropertyPermission class** 62, 114  
**protection domains**  
     *See also* ProtectionDomain class  
     access control  
         basic algorithm 94–97  
         extended algorithm 98–101  
         full algorithm 107–109  
     combining 91–92

    creating 75–77  
     system domain 78, 94  
     types 94  
**ProtectionDomain class** 50–51, 74–79, 152  
     *See also* protection domains  
**protocol, secure socket** 255  
**Provider class** 188, 273  
**providers**  
     *See also* Provider class  
     adding 273–274  
     configuring 273–274  
     installing 271–272  
     master class 273  
     overview 179–180  
     Policy 120–124  
     preference order 181, 273  
     SUN 185–187, 203, 207, 232–233  
     SunJCE 186–187, 209, 214, 216, 220  
     SunJSSE 254, 256–259  
**pseudo-random-number generator (PRNG)** 206–207  
**public fields, security issues** 158, 160  
**public key** 15  
**public methods, security issues** 158, 160  
**public-key certificates**  
     *See* digital certificates  
**public-key cryptography** 138  
**PublicKey interface** 197

**Q**

**QOP (quality-of-protection)** 249

**R**

**Rabin, M. O.** 13  
**Random class** 206  
**random-number generation** 206–208  
     algorithm standard names 232  
**RC2 cipher algorithm** 234  
**RC4 cipher algorithm** 234  
**RC5 cipher algorithm** 234  
**readObject method** 163–167  
**readPasswd method** 228  
**readResolve method** 165  
**ReflectPermission class** 62, 68  
**refresh method** 81–82  
**Remote Method Invocation (RMI)** 260–263  
**Remote Procedure Call (RPC)** 19  
**removeProvider method** 187

- replay detection 248
- requestCredDeleg method 244
- requestPasswordAuthentication method 153
- resolveClass method 47, 49
- RFC 2104 179
- RFC 2587 133
- RFC 2743 154
- RFC 3280 137
- RFC 822 140
- Rivest, R. L. 13
- RMI (Remote Method Invocation) 260–263
- root certificate 16
- RPC (Remote Procedure Call) 19
- RSA
  - description 231
  - key-pair generation algorithm specification 240
  - standard algorithm name 231, 234
  - usage 16
- RSA-based signature algorithms 238
- RSAMultiPrimePrivateCrtKeySpec class 199
- RSAPrivateCrtKeySpec class 198
- RSAPrivateKeySpec class 198–199
- RSAPublicKeySpec class 199
- run method
  - PrivilegedAction interface 100–105, 107, 151
  - PrivilegedExceptionAction interface 151
- RuntimePermission class 60, 62, 113–114
- S**
- S/MIME protocol 133
- sandbox model 25, 33
  - limitations of 32
- SASL (Simple Authentication and Security Layer Application Programmer's Interface) 143
- Schilling, M. 13
- SDK from JDK terminology shift 30
- SDSI certificates 134
- SealedObject class 171–172
- secret keys 12, 14, 16–17, 178, 216, 219
- secret-key ciphers 14
- secret-key factory algorithm standard names 236
- SecretKey interface 217, 219
- SecretKeyFactory class 216–217
  - programming example 229
- SecretKeySpec class 217
- secure socket protocol 255
- SecureClassLoader class 43–53
- SecureRandom class 206–208
  - programming example 222
- security
  - architecture
    - See architecture, security
  - attack types 3
  - basic features of Java security 23–30
  - exceptions 157–158
  - fundamentals 1–21
  - manager
    - See also SecurityManager class
    - example use 88
    - installation 89, 271
  - models 8–12
  - network 241–263
  - of objects 157–176
  - policy
    - See policy
  - properties
    - See properties
  - properties file 121, 268–269
  - tools 289–306
  - versus cryptography 2, 12
- Security class 187–188
- security.overridePropertiesFile security property 270
- security.provider.*n* security property 273
- SecurityException class 82, 158
- SecurityManager class 87–90, 92
  - See also security manager
  - checkPermission methods 89–90
  - default implementation 150
  - subclassing examples 118–120
  - versus AccessController class 109–110
- SecurityPermission class 62
- seeds for random-number generators 206–208
- self-signed certificate 16, 297
- sequencing 248
- Serializable interface 163–168, 171
- SerializablePermission class 62
- serialization 163–167
- ServerSocketFactory class 250
- service attribute standard names 233
- service provider
  - See providers

*Index*

- Service Provider Interface (SPI)** 184
  - ServicePermission class** 154–155, 245–247
  - setCertificateEntry method** 205
  - setDefaultSSLSocketFactory method** 253
  - setEnabledProtocols method** 255
  - setKeyEntry method** 205
  - setPolicy**
    - method 81–82
    - permission 81
  - setProperty method**
    - Security class 188
    - System class 267
  - sets of permissions** 66–67
  - setSecurityManager**
    - method 89
    - permission 89
  - setSeed methods** 207, 222
  - setSigners method** 51
  - setSSLSocketFactory method** 253
  - setting property values**
    - security 268–269
    - system 267
  - SHA-1 message digest algorithm**
    - programming example 220–222
    - specification 238
    - use in HMAC 179
  - SHA1PRNG pseudo-random-number generation algorithm** 232
  - SHA1withDSA signature algorithm** 238
  - SHA1withRSA signature algorithm** 238
  - SHA-256 message digest algorithm** 231
  - SHA-384 message digest algorithm** 231
  - SHA-512 message digest algorithm** 231
  - Shannon, Claude** 12
  - sign method** 191, 223
  - signature**
    - See* digital signature
  - signature (instructions) file** 140, 302
  - signature block file** 140, 302
  - Signature class** 169, 184, 190–192, 222–224
  - SignatureSpi class** 184
  - signed code** 29–30, 138–141
  - signedBy** 277–280
  - SignedObject class** 168–171
  - Simple Authentication and Security Layer Application Programmer's Interface (SASL)** 143
  - Simple Public Key Mechanism (SPKM)** 143
  - single sign-on** 144, 245
  - smart cards** 19
  - socket factories** 251
  - SocketFactory class** 250
  - SocketPermission class** 113
  - spanning permissions** 86, 124
  - SPI (Service Provider Interface)** 184
  - SPKI** 144
  - SPKM (Simple Public Key Mechanism)** 143
  - SQLPermission class** 62
  - SSL protocol** 133, 155
  - SSL3Padding** 235
  - SSLContext class** 250, 252, 254–256
  - SSLPermission class** 62
  - SSLServerSocket class** 250–251
  - SSLServerSocketFactory class** 250–252
  - SSLSession interface** 250, 252
  - SSLSocket class** 250–252
  - SSLSocketFactory class** 250–253, 255
  - stacked authentication** 146
  - standard names** 230–237
  - static fields, security issues** 160
  - store method** 205
  - subject**
    - See also* Subject class
    - defined 143–144
    - digital certificate 131–132
  - Subject class** 144–152, 154
  - SubjectDomainCombiner class** 125
  - SUN provider** 185–187, 203, 207, 232–233
  - SunJCE provider** 186–187, 209, 214, 216, 220
  - SunJSSE provider** 254, 256–259
  - symmetric cipher** 14
  - System class** 89
  - system classes** 43, 55–56, 78
  - system domain**
    - See* protection domains
  - system properties**
    - See* properties
- T**
- tainted variables** 163
  - target name, permissions** 60
  - terminology shift from JDK to Java 2 SDK** 30

**TGS (Ticket Granting Service)** 246  
**TGT (Ticket Granting Ticket)** 154  
**Ticket Granting Service (TGS)** 246  
**Ticket Granting Ticket (TGT)** 154  
**TLS protocol** 133  
**toString method** 60–61  
**transformation** 208–209  
**transient keyword** 166  
**transparent key representation** 196–197, 216  
**transparent parameter representation** 192  
**Triple DES**  
    *See* DES-EDE  
**triple-DES** 14  
**Trojan horse** 9  
**trust anchor** 128  
**trust manager** 254, 256, 258  
    *See also* TrustManager interface  
**trust, establishing** 127–156  
**TrustAnchor class** 136  
**trusted certificate entry** 155, 290, 294  
**Trusted Third Party (TTP)** 132  
**TrustManager interface** 250, 256  
    *See also* trust manager  
**TrustManagerFactory class** 250, 256–258  
**truststore** 155  
**type safety** 27–29  
**type-safe linkage** 41

## U

**UnresolvedPermission class** 64–66  
**unwrap method** 212, 249  
**update method**  
    Cipher class 211, 214  
    Mac class 220  
    MessageDigest class 189, 221  
    Signature class 191, 223–224  
**URL (Universal Resource Locator)** 69  
**URLClassLoader class** 43–44, 49, 53–54  
**user.home system property** 268  
**user-centric access control** 142  
**user-centric authentication and authorization** 141–152

## V

**validate method** 136  
**variables, tainted** 163  
**verify method** 170, 191, 223–224  
**verifyMIC method** 249

**VPN (virtual private network)** 5–6

## W

**Wilkes, M. V.** 13  
**wrap method** 211, 248–249  
**writeObject method** 164

## X

**X.500 directory** 128  
**X.500 distinguished names** 306–307  
**X.509**  
    certificate type 232  
    certificates 128, 132, 134, 136, 201, 256, 258  
    extensions 134  
    key format 197, 200  
**X500Principal class** 283, 306  
**X509Certificate class** 134, 201  
**X509CRL class** 134, 201  
**X509CRLEntry class** 134  
**X509EncodedKeySpec class** 200, 224  
**X509Extension interface** 134

## Y

**Yellin, F.** 29  
**Yung, M.** 13