

index

Symbols

.. 52
// 52

Numerics

3DES 216, 240, 247
403 Authorization Required 87

A

acceptSecContext 195
access control context 192
Access Control List. *See* ACL
access control. *See* authorization
ACL 16
Action 121
Active Directory 196, 206
 ktpass utility. *See* ktpass
actor 64, 94–95, 108, 122–123
AES 217, 240
AlgorithmSuite 387
ancestor:: 52
Ant 36–38, 70, 198
AON 5, 30, 32, 119, 427, 430, 473
Apache Axis 85
 See also Axis
Apache Axis. *See* Axis
Apache Neethi 396
Apache Rampart. *See* Rampart
Apache Software Foundation 35
Apache WSS4J. *See* WSS4J

Apache XML Security 246, 259, 287
application layer 87, 89
application level security 90
Application-Oriented Networking. *See* AON
AppliesTo 348
AquaLogic 30
AS, Kerberos 184
AS2 54
Assertion 326, 464
AssertionId 462
AsymmetricBinding 386
attachment 367
 See also SwA
attack 13, 20
 brute force 215
 buffer overflow 434, 444
 chosen text 215
 distributed denial of service (DDoS) 436
 forgery 462
 frequency analysis 215
 known text 215
 man in the middle (MIM) 263
 message tampering 220
 replay 176, 462, 465
 repurposing 174, 177, 320, 465
 social engineering 400
 SQL injection 435
 XML specific 438, 444
 entity recursion 438, 444
 external entity 439, 444

AttributeStatement 328
authentication 13–14, 26, 205
 at application layer 88
 delegatable 176–177, 186
 HTTP Basic 87
 HTTP Digest 87
 at HTTP layer 87
 IP-address based 87
 multifactor 175, 401
 mutual 176, 186
 password based. *See* password
 SSL-certificate based 87
 at transport layer 87
 via encryption 180
 in web applications 87
Authentication Service. *See* AS
AuthenticationStatement 327
authorization 13, 16, 26
AuthorizationDecisionQuery 352
AuthorizationDecisionStatement 329, 353
availability 433
Axis 29, 35, 68
 Axis2 49, 83
 consuming a service 72
 creating a web service 68
 getting started 36
 handler 103
 message-style service 338
 RPC-style service 338
 using HTTPS as transport 233
 WSDD. *See* WSDD

B

base64 285, 289
 base64 encoding 155, 159
 RFC 172
 BEA AquaLogic. *See* AquaLogic
 BEA WebLogic. *See* WebLogic
 BEA WebLogic Server. *See*
 WebLogic
 BinarySecurityToken 199, 201,
 278, 286, 289
 binding. *See* wsdl binding
 Body 48
 BPM 407
 branch office 418
 Business Process Management.
 See BPM

C

C# 76
 c14n. *See* canonicalization
 CA 224–230, 256, 279, 283,
 290, 394
 caching 430
 Caesar shift 215
 Call 74
 CallbackHandler 140–141, 148
 canonicalization 266, 281
 choosing between inclusive
 and exclusive 303
 exclusive 271
 specification 305
 inclusive 271
 specification 305
 CanonicalizationMethod 280,
 291
 certificate 98, 171, 224, 262
 chain 226, 278, 283
 self-signed 229
 Certificate Authority. *See* CA
 Certificate Signing Request. *See*
 CSR
 Certification Revocation List.
 See CRL
 CertPath 285
 CertPathValidator 299
 checksum 220
 chroot 20, 444
 CICS 443
 CipherData 240

CipherReference 240
 CipherValue 240
 Cisco AON. *See* AON
 Code 64
 Comment 50
 composite service 413
 ComputedKey 351
 com.sun.security.auth.module
 145
 confidentiality 13, 17, 471
 context 102
 context-independent 8
 CORBA 54, 64, 407
 CRL 300
 cryptography 259
 CSR 230
 current access control
 context 192

D

data center 417, 420
 DataPower 30, 32
 DataReference 243
 DCOM 54
 DDoS 436–437, 439
 declarative security 358
 decryption. *See* encryption
 deployment architecture 414
 DES 216
 See also 3DES
 descendant:: 52
 detail 63, 96
 Dialect 375
 digest 264
 message 220
 password digest. *See* password
 DigestMethod 280
 DigestValue 280
 DII 72, 74
 DIME 457, 460
 Direct Internet Message Encap-
 sulation. *See* DIME
 discoverable 8
 distinguished name. *See* DN
 Distributed Component Object
 Model. *See* DCOM
 distributed computing 54
 distributed denial of service. *See*
 DDoS
 DMZ 423

DN 224
 doAs 192
 Document 50
 document exchange 80
 Document Object Model. *See*
 DOM
 Document Type Definition. *See*
 DTD
 DOM 49–50, 82
 DTD 46, 82, 243, 268–269,
 275, 438–439
 Dynamic Invocation Interface.
 See DII
 dynamic proxy 72–73

E

ebXML 54
 EDI 54
 EJB 68, 77–78
 Element 50
 encoding 64, 80, 95–96
 encodingStyle 58, 95–96
 EncodingType 278
 EncryptedData 239
 EncryptedElements 393
 EncryptedKey 239, 241, 255
 EncryptedParts 393
 encryption 471
 basics 178, 214
 block oriented 216
 hybrid 222
 java API 235
 mixing with signatures
 303
 practical issues 256
 public key 218
 of SOAP messages 237
 stream oriented 216
 symmetric key 216
 of XML. *See* XML Encryption
 EncryptionMethod 240
 EndorsingSupportingToken
 391
 EndpointReference 347
 endpoints 60, 85, 119,
 318–325, 382
 legacy 355
 Enterprise JavaBean. *See* EJB
 enterprise resource planning.
 See ERP

Enterprise Service Architecture.
See ESA
 Enterprise Service Bus.
See ESB
 Entropy 347
 Envelope 48
 ERP 412, 443
 ESA 443
 ESB 8, 27, 30, 125
 ethereal 211
 eXtensible Access Control
 Markup Language. *See*
 XACML
 eXtensible Markup Language.
See XML
 eXtensible Schema Definition.
See XSD

F

FailedAuthentication 99
 FailedCheck 99
 fault 61
 SOAP 1.1 61
 faultactor 63
 faultcode 61
 defined by WS-Security 99
 faultstring 63–64
 firewall 20, 422, 444
 following:: 52
 Forum Systems 32
 FTP 56, 89

G

General Security Services API.
See GSS API
 Java bindings of. *See* JGSS
 GetMetadata 375
 governance 6
 GSS API 189
 Java bindings RFC 207
 RFC 207
 GSSManager 190
 GSSName 190

H

handle, in CallbackHandler
 142
 handleFault 106, 112, 114

handler 85, 102–103, 124–125
 chaining 112
 client-side 110
 configuration 114
 client-side 116
 server-side 114
 initialization 106
 JAX-WS enhancements 127
 .Net equivalent
 SOAPExtension. *See* .NET
 server-side 106
 handleRequest 106, 108, 112
 handleResponse 106, 112, 114
 Header 48, 94
 header 91–93
 anatomy of 93
 entry 93
 standard attributes 94
 href 60
 HTTP 22, 56, 89
 HTTP Basic Authentication. *See*
 authentication
 HTTP Digest Authentication.
See authentication
 HTTP layer 87
 HTTP proxy 118
 HTTPS 213, 231
 with Tomcat 231

I

IBM DataPower. *See* DataPower
 IBM MQ Series. *See* MQ Series
 IBM Websphere. *See* Websphere
 ID 43, 243, 366
 Id 243, 283, 366, 462
 identifier reference. *See* IDREF
 identity claim 132
 IDL 64
 IDREF 43, 366
 InclusiveNamespaces 273,
 304
 init
 javax.xml.rpc.handler.
 Handler 106
 javax.xml.rpc.server.Service-
 Lifecycle 110
 InitiatorToken 386
 initSecContext 193
 integrity 13, 19
 integrity. *See* message integrity

Interface Definition Language.
See IDL
 intermediaries 85, 91, 94,
 118–119, 121, 322, 331
 interoperability 13, 22, 56, 75,
 80, 361, 363, 365
 intranet 417
 intrusion detection 20–21
 InvalidSecurity 99
 InvalidSecurityToken 99

J

J2EE 24, 35
 JAAS 138, 189
 CallbackHandler. *See*
 CallbackHandler
 configuration 143
 LoginContext. *See* Login-
 Context
 LoginModule
 for Kerberos 195, 208
 for keystores 285
 LoginModule. *See* Login-
 Module
 reference 172
 Java API for XML based RPC.
See JAX-RPC
 Java API for XML Messaging.
See JAXM
 Java API for XML Processing.
See JAXP
 Java API for XML Registries.
See JAXR
 Java Authentication and Autho-
 rization Service. *See* JAAS
 Java Certification Path API 285
 Java Community Process. *See*
 JCP
 Java Cryptographic Extension.
See JCE
 Java Cryptography Architecture.
See JCA
 Java Development Kit. *See* JDK
 Java Messaging Service. *See* JMS
 Java Specification Request. *See*
 JSR
 Java2WSDL 69–70
 java.rmi.Remote 69
 java.rmi.RemoteException 69,
 114

- java.security.auth.login.config 143, 198
 - java.security.cert 285, 298
 - java.security.KeyStore 235
 - java.security.krb5.kdc 193, 198
 - java.security.krb5.realm 198
 - java.security.MessageDigest 158
 - java.security.SecureRandom 158
 - javax.crypto.Cipher 236, 246
 - javax.xml.namespace 105
 - javax.xml.rpc.Call. *See* Call (javax.xml.rpc.Call)
 - javax.xml.rpc.handler 105
 - javax.xml.rpc.handler.GenericHandler 106
 - javax.xml.rpc.handler.Handler 106
 - javax.xml.rpc.handler.Handler-Info 106
 - javax.xml.rpc.handler.MessageContext. *See* MessageContext
 - javax.xml.rpc.handler.soap 105
 - javax.xml.rpc.Stub 73
 - See also* Stub
 - javax.xml.soap 105
 - JAXM 35, 339
 - JAXP 105
 - JAXR 81, 83
 - JAX-RPC 35, 69, 82, 105, 112, 126
 - handler. *See* handler
 - JAX-WS 82
 - JCA 78, 285
 - JCE 235, 248, 258
 - JCEKS 235
 - JCP 35, 82
 - JDK 228
 - JGSS 175, 189, 207
 - JKS 235
 - JMS 56, 78, 89, 407
 - JSR-105 305
 - JSR-106 257, 259
 - JUnit 36
- K**
-
- KDC. *See* Kerberos
 - Kerberos 29, 98, 171, 174, 319, 366, 468
 - Authentication Service (AS) 184
 - introduction 177
 - KDC 180
 - with Microsoft Active Directory 196
 - logon session key 184
 - long-term key 180
 - proxy ticket 186
 - RFC 207
 - session key 181
 - TGS 184
 - TGT 184
 - with WS-Security 199
 - key
 - alias 228
 - private 218
 - public 218, 247
 - store 228
 - Key Distribution Center. *See* Kerberos
 - KeyGenerator 248
 - KeyIdentifier 463–464
 - KeyInfo 241, 253, 282, 286, 290
 - KeyStoreLoginModule 285
 - keytab 197
 - keytool 228, 259
 - KRB_AP_REQ 194
 - GSS-wrapped 203
 - Krb5LoginModule, LoginModule for Kerberos. *See* JAAS
 - ktpass 197, 208
- L**
-
- Layer 7 30, 32
 - Layout 389
 - LDAP 15, 27, 138, 205, 410, 420
 - Lightweight Directory Access Protocol. *See* LDAP
 - LoginContext 140, 145, 193
 - LoginModule 139
 - for digest authentication 163
 - implementing 145
- M**
-
- MAC 261, 282
 - manageability 6, 13, 23
 - MemberOfGroupPrincipal 141
 - Message Authentication Code. *See* MAC
 - message integrity 220, 261
 - message level security 25, 90, 366
 - message queue. *See* MQ
 - MessageContext 69, 107, 109–110, 112, 141, 296
 - MIME 454
 - RFC 460
 - MQ 89
 - Series 407
 - MQ providers. *See* JMS, MQ Series
 - MTOM 454, 458, 460
 - multiRef 59
 - mustUnderstand 94, 96, 123–124
- N**
-
- NameCallback 142
 - namespace 43, 82, 269
 - default 44
 - NAT 424
 - .NET 29, 31, 35, 75, 396
 - SOAPExtension 103, 118, 127
 - WSE 31, 396
 - Network Address Translation. *See* NAT
 - Node 50
 - NodeList 51
 - nonce 152, 158, 470
 - nonrepudiation 19
 - NotUnderstood 96
- O**
-
- OASIS 31, 92
 - OID 191
 - one-way function 152
 - OpenSAML 331, 355
 - optional JAAS keyword 143
 - org.apache.xml.security 287
 - org.apache.xml.security. encryption 246
 - org.ietf.jgss 189
 - org.w3c.dom 50

P

PAM 138
 password 133
 digest 151, 168
 problems 169
 validating 161
 limitations 170
 PasswordCallback 142, 147
 performance 429
 PKI 174, 206, 222, 256, 262
 PKIPath 278, 285
 PkiPath 289
 Pluggable Authentication
 Model. *See* PAM
 policy 370
 fetching 374
 intersection 371, 373
 policy-driven security 25, 28
 PolicyReference 378
 port type. *See* wsdl
 portType
 preceding:: 52
 prefix 43, 270
 rebinding 44
 See also namespace
 principal 141, 197
 privacy 13, 21, 462, 471
 PrivilegedAction 193
 profile 98
 provisioning 24
 pseudonyms 471
 public key infrastructure. *See*
 PKI

R

Rampart 29, 32
 RBAC 16
 RC2 217
 RC4 217
 RC5 217
 Reactivity 30, 32
 Reason 64
 RecipientToken 387
 Reference 280, 282, 286,
 290–291, 451, 463
 ReferenceList 241, 250, 252
 RELAX NG 46, 82
 relay 96, 123
 Remote Procedure Call. *See* RPC

replication 431
 repudiation 261
 repurposing. *See* attack
 RequestedAttachedReference
 349
 RequestedProofToken 350
 RequestedUnattachedReference
 350
 required JAAS keyword 143
 RequiredElements 393
 requisite JAAS keyword 143
 role 64, 94, 96, 108, 122
 Role-Based Access Control. *See*
 RBAC
 RosettaNet 54, 60
 RPC 55, 57, 80
 RSA 218, 240, 242, 247
 RSTR 346

S

SAAJ 35, 105
 SAML 28–29, 273, 325, 366,
 410, 431
 Assertion. *See* Assertion
 Protocol 343, 352
 specification 355
 SAMLAuthorityBinding
 350
 SAP R/3 443
 Sarvega 32
 SAX 82
 scalability 431
 schema 45, 82, 243
 SecretKey 248
 Secure Shell. *See* SSH
 Secure Sockets Layer. *See*
 SSL/TLS
 security
 claim 97
 context 79, 90, 315
 framework 406
 gateway 427
 model 99
 policy 360
 token 98
 Security as a service 25–26
 Security Assertion Markup
 Language. *See* SAML
 Security header entry 97–98,
 100
 security service 315
 use cases 316
 Security Token Service. *See* STS
 SecurityContextToken 450
 SecurityTokenReference 241,
 282, 290, 389, 463
 SecurityTokenUnavailable 99
 self-describing 8
 Service
 composition 413
 definition 7
 Service
 (javax.xml.rpc.Service) 75
 service design choices 77–80
 service level agreement. *See* SLA
 service provider abuse
 repurposing. *See* attack
 Service-Oriented Architecture.
 See SOA
 session key. *See* Kerberos
 SHA-1 152, 158, 169, 220
 specification 172
 SHAIPRNG 158
 sibling:: 52
 Signature 279, 286–287, 464
 SignatureMethod 280, 291
 SignatureValue 286
 SignedElements 393
 SignedEndorsingSupporting-
 Token 391
 SignedInfo 279, 286, 291, 463
 SignedParts 392
 SignedSupportingToken 391
 signing 220, 262, 286
 practical issues 302
 Simple API for XML. *See* SAX
 Single Sign-On. *See* SSO
 SLA 404
 SMTP 89, 91
 SOA 31
 introduction to 4–10
 SOAP 10, 25, 85
 1.1 56
 specification 82
 1.2 56
 specification 82
 alternatives 78
 basics 55
 Body. *See* Body
 document exchange 60
 encoding 59

- SOAP (*continued*)
 Envelope. *See* Envelope
 Extensions 124
 fault. *See* fault
 Header. *See* Header
 layer 89
 level security 91
 Message Transmission Optimization Mechanism. *See* MTOM
 RPC 57
 with Attachments API for Java. *See* SAAJ
 with Attachments. *See* SwA
 XSD for 1.1 47
 SOAPAction 58, 66, 121
 SOAPConnection 340
 soapenc root 60
 soapenv
 Client 62
 DataEncodingUnknown 64
 MustUnderstand 62
 Receiver 64
 Sender 64
 Server 62
 VersionMismatch 62
 SOAPEnvelope 339
 SOAPFaultException 114
 SOAPMessage 339
 SOAPMessageContext 339–340
 Sorbanes-Oxley Act 310
 SSH 90
 SSL 87, 89, 151, 231, 468
 limitations 234
 SSL/TLS 17–19, 22, 25
 SSO 88, 90, 176–177, 207
 StAX 49, 82–83
 STR dereference transform 464
 STR. *See* SecurityTokenReference
 streaming 49
 Streaming API for XML. *See* StAX
 STS 344–345, 366
 Stub 72, 117
 Subcode 64
 Subject 191, 328
 SubjectConfirmation 468
 holder-of-key 469
 sender-vouches 468
 SubjectKeyIdentifier 366, 389
 sufficient JAAS keyword 143
 SupportingTokens 391
 SwA 454
 limitations 457
 specification 460
 SymmetricBinding 383
- T**
-
- targetNamespace 48
 TCP 89
 tcpmon 38
 Text 50
 TGS. *See* Kerberos
 TGT. *See* Kerberos
 TIBCO 407
 ticket 182
 timestamp 367, 470
 TLS 151, 212, 231, 468
 limitations 234
See SSL/TLS
 To 121
 TokenType 347
 Tomcat 36
 HTTPS configuration 231
 Transform 280
 transport layer 25, 87, 89–90, 366
 Transport Layer Security. *See* SSL/TLS
 TransportBinding 383
 TripleDES. *See* 3DES
 turnkey security profiles 29
- U**
-
- UBR 80
 UDDI 10, 80, 83, 376
 Uniform Resource Identifier. *See* URI
 Uniform Resource Locator. *See* URL
 Universal Business Registry. *See* UBR
 Universal Description, Discovery, and Integration. *See* UDDI
 UnsupportedAlgorithm 99
 UnsupportedCallbackException 148
 UnsupportedSecurityToken 99
 URI 43
 URL 44
 URLEndpoint 340
 UsernamePrincipal 141, 204
 UsernameToken 98
 processing 148
 specification 172
 with password digest 154
 UTF-8, RFC 172
- V**
-
- validity 46
 ValueType 242, 278, 451, 463–464
 VeriSign 227, 230
 Visual C#.NET 76
 Visual Studio .NET 76
 VPN 468
 vulnerability 20–21, 26
 vulnerability management 433
 remediation workflow 440
- W**
-
- W3C 31
 WCCP 473
 web application 86
 Web Cache Coordination Protocol. *See* WCCP
 web Service definition 10
 Web Service Deployment Descriptors. *See* WSDD
 Web Services Enhancements. *See* WSE
 WebLogic 29, 31, 35, 396
 WebServices Description Language. *See* WSDL
 WebSphere 30, 35
 well-formed 41, 46
 Windows CardSpace 355
 WinPcap 211
 WLS. *See* WebLogic
 WS-Addressing 85, 119, 322, 334
 specification 127
 WSDD 114, 338
 WSDL 10, 64, 69–70, 72, 78–79, 83, 375

- wsdl
 - Binding 377
 - binding 66
 - definitions 65
 - message 67
 - operation 67
 - Port 377
 - port 65
 - PortType 377
 - portType 67
 - types 68
 - WSDL2Java 70, 72
 - WSE 29, 31, 396
 - WS-I 56, 83, 457
 - Attachments Profile 460
 - Basic Profile 56, 83
 - Basic Security Profile specification 395
 - Basic Security Profile 368
 - WSIF 78, 83
 - WS-MetadataExchange 355, 375
 - specification 395
 - WS-Policy 31, 99, 369, 372
 - specification 395
 - WS-PolicyAssertions 373
 - WS-PolicyAttachment 348
 - specification 395
 - WS-ReliableMessaging 369
 - WSS4J 29, 31
 - WS-SecureConversation 379, 431, 452
 - WS-Security 25, 85, 92, 99
 - introduction 97
 - Kerberos Token Profile 208
 - SAML Token Profile 355
 - specification 127
 - SwA Profile 457, 460
 - UsernameToken Profile 172
 - with Kerberos 199
 - X.509 Certificate Token Profile 283
 - WS-SecurityPolicy 28–29, 348, 355, 373, 379
 - specification 395
 - WS-Trust 28, 343–344, 355, 366, 379
 - specification 355
 - wsu Id 243, 275, 279, 366, 450, 462
- X**
-
- X.509 98, 224
 - certificate. *See* certificate
 - X509 242
 - X509Certificate 250
 - X509IssuerName 241, 389
 - X509IssuerSerial 241, 389
 - X509SerialNumber 242, 390
 - XACML 394
 - XFire 83
 - XML 10
 - 1.1 specification 82
 - basics 39
 - encryption. *See* XML Encryption
 - namespace. *See* namespace
 - parsing 49
 - schema. *See* schema
 - signature. *See* XML Signature
 - validity. *See* validity
 - vocabulary 46
 - well-formed. *See* well-formed
 - xml
 - base 122
 - id 243, 273, 305, 366
 - lang 64, 273
 - space 273
 - XML Canonicalization. *See* canonicalization
 - XML Encryption 237, 248, 259
 - XML Schema Definition. *See* XSD
 - XML Signature 277
 - specification 305
 - XMLCipher 246, 255
 - XML-RPC 54
 - XMLSignature 287, 291
 - XOP 458, 460
 - XPath 51, 82, 243, 246, 284, 431
 - XPointer 243, 294
 - XSD 46, 375
 - for SOAP 1.1 47