Index

A
Apache Directory Server
  Apache Tomcat, 41
  configuration, 39–41
Apache Tomcat, enable TLS, 43
Application programming interface (API), 1
definition of, 3
  JDBC, 1
  vs. Managed APIs, 3
  marshalling/unmarshalling technique, 2
ProgrammableWeb, 3
for remote access, 2
RESTful services, 3
  vs. service, 4
SOAP-based web services, 2
UDDI, 5
  WS-Discovery, 5
Assertion, 173
Authentication vs. authorization, 131
Authorization API token (AAT), 165

B
Brokered authentication, 171
  authorization server, 172
  OAuth client applications, 172

C
Chain grant type profile, 149
  authorization server, 149
  resource server, 150
  scope parameter, 150
cURL command
  Flickr authentication, 68
  Google AUTHSUB, 65
  Google ClientLogin, 63
  Yahoo! BBAuth, 71

D
Delegated access control, 222
  hidden credentials, 229
  Proxy identity, 223–224
  STS, 228–229
  with JWT, 224–225
Dynamic client registration, 150

E
eXtensible Access Control Markup Language (XACML), 144, 228
  architecture, 145
  runtime execution, 145
  target element, 148
Token introspection profile
  API gateway, 147
  attribute mapping, 147
  security gateway, 147

F
Facebook, 109–110
  access token, 111
  client registration, 110
  Page access token, 114
  user access token, 112
Federation, 171
  brokered authentication
    (see Brokered authentication)
    identity management systems, 171

G
Google
  application authentication, 126
  authorization code, 124
  client registration, 124
Google (cont.)
device authentication, 129
implicit code, 128

■ H
Hash-based Message Authentication Code (HMAC), 139
HTTP Basic authentication, 33
API security, 42
GitHub API, 33
HTTP Digest Authentication, 33
vs. Basic Authentication, 36
limitations, 34
message-related data, 36
multiple algorithm support, 36
nonce, 35
opaque, 35
quality of protection, 35
realm, 35
Recipe API security, 45
RFC 2617, 36
security-related data, 36

■ I
Identity delegation model, 59
brokered delegation, 60
Google Drive, 60
Lucidchart account, 60
direct delegation, 59
Flickr account, 59
Snapfish, 59
Flickr Authentication, 67
Google AuthSub, 65
Google ClientLogin, 62
internet engineering task force (IETF), 72
internet identity workshop (IIW), 73
roles, 59
SlideShare, 61
twitter, 60
web resource authorization profiles (WRAP), 73
Yahoo! BBAuth, 70
Integrated Windows Authentication (IWA), 223
Internet Assigned Numbers Authority (IANA), 202
Internet engineering task force (IETF), 72

■ J, K, L
JSON Web Encryption (JWE), 201, 213
attributes, 214–215
content encryption vs. key wrapping, 215
header, 214
serialization, 220
attributes, 216
data structure, 215–216
Java coding, 217–218
PublicKey, 218–219
JSON Web Signature (JWS), 201, 206, 225
algorithms, 207
attribute, 206–207
serialization
attributes, 208
coding implementation, 208
definition, 208
Java coding, 209–212
JSON payload, 210
PrivateKey, 213
specification, 206
JSON Web Token (JWT), 180, 201
claim set, 202
definition, 201
Java code, 203–205
JOSE header, 201, 205
OpenID connect, 201
private claims, 203
public claims, 203
registered claims, 202

■ M, N
MAC token profile, 133, 135
audience parameter, 136
authentication, 138
authorization code
client application, 135
cURL command, 136
grant type, 135–136
HTTP header, 135
parameters, 137
bearer tokens, 134
calculation, 138
Expiring tokens, 134
grant types, 134, 141
HMAC, 139
HTTP Request-Line, 139
OAuth 1.0 vs. OAuth 2.0, 141
resource server, 140
unbounded tokens, 134
working principles, 133
Managed APIs, 1
Salesforce API, 8
Twitter API, 6
Message authentication
code (MAC), 139

■ O
OAuth
MAC token profile (see MAC token profile)
three-legged vs. two-legged, 88
token based authentication (see Token-based authentication)
WRAP, 89 (see also Web resource authorization profiles (WRAP))
OAuth 1.0 vs. OAuth 2.0, 103
OAuth 2.0, 91
client types
  confidential clients, 103
  public clients, 103
Facebook, 109
  access token, 111
  client registration, 110
  Page access token, 114
  user access token, 112
Google, 124
  application authentication, 126
  authorization code, 124
  client registration, 124
  device authentication, 129
  implicit code, 128
LinkedIn, 116
  access token, 117
  client registration, 117
Recipe API, 104
  authorization code, 105
  client credentials, 108
  implicit code, 107
  resource owner password, 107
refresh token, 109
salesforce, 119
  authorization code, 120
  client registration, 119
  implicit code, 122
  resource owner password, 123
WRAP (see Web resource authorization profiles (WRAP))
OpenID Connect, 181
  Amazon, 183
  API security, 199
  directed identity, 182
  dynamic client registration, 197
  flow chart representation, 194
  google, 192
  grant types, 191
  identity provider metadata, 196
ID token, 184
  attributes, 184
  JSON web encryption (JWE), 185
  JSON web signature (JWS), 185
  JSON web token (JWT), 184
overview, 181
protocol flow, 182
relying party, 181
request attributes, 187
user attributes, 189, 191
WebFinger protocol, 194
  identity provider, 196
  rel parameter, 195
  resource parameter, 195
WSO2 Identity Server, 185

Patterns, 221
  chained access delegation, 226
  delegated access control
    hidden credentials, 229
    Proxy identity, 223–224
    STS, 228–229
    with JWT, 224–225
  nonrepudiation, 225
  Single Sign-On (SSO)
    delegated access control, 222
    IWA, 223
    trusted master access delegation, 227–228
  Trusted Subsystem, 221
  Perfect forward secrecy (PFS), 56
  Policy Enforcement Point (PEP), 228
Profiles, 143
  chain grant type, 149
  dynamic client registration profile, 151
  token introspection
    (see Token introspection profile)
    token revocation, 152

Recipe API deployment, Apache Tomcat, 37
Requesting party token (RPT), 164

Secure Transport Layer Protocol (STLP), 47
Security, 11
  auditing, 21
  authentication, 18
  authorization, 19
  availability, 16
  Brokered Authentication pattern, 26
  complete mediation, 14
  confidentiality, 14
  message-level encryption, 15
  SSL bridging, 15
  TLS tunneling, 15
  DAC vs. MAC, 19
  defense in depth, 12
Security (cont.)
- Direct Authentication pattern, 22
- biometric authentication, 24
- limitations, 22
- managing credentials, 23
- yellow zone, 22
- fail-safe defaults, 13
- insider attacks, 12
- integrity, 16
- Kerckhoff’s principle, 13
- least common mechanism pattern, 14, 26
- least privilege principle, 13
- nonrepudiation, 21
- open design, 14
- performance, 11
- policy-based access control pattern, 27
- psychological acceptability, 14
- sealed green zone pattern, 25
- separation of privilege, 14
- simplicity, 13
- threat modeling, 29
- user comfort, 11
- weakest link, 12

Security Assertion Markup Language (SAML), 173
- client authentication, 174
- grant type
  - brokered authentication, 177
  - identity provider, 176
  - JWT profile, 180
  - out of band, 177
  - WSO2 identity server, 177

Security Token Service (STS) pattern, 228
System for Cross-domain Identity Management (SCIM) working group, 205

Token revocation profile, 152
Transport Level
- Security (TLS), 206, 222

Token-based authentication, 75–76
- resource-owner authorization phase, 78
- secured business API, 80
- signature methods, 80
  - HMAC-SHA1, 83
  - PLAINTEXT, 81
  - RSA-SHA1, 83
- temporary-credential request phase, 76
  - authorization header, 77
  - client-registration process, 77
  - token-credential request phase, 79
- twitter APIs, 85
- unique identifier, 75

Token introspection profile, 143
- HTTP authentication, 143
- JSON response, 144
- validation, 144

XACML, 144
- API gateway, 147
- architecture, 145
- attribute mapping, 147
- runtime execution, 146
- security gateway, 146
- Target element, 148

U, V

Universal Description, Discovery and Integration (UDDI), 5
User managed access (UMA), 155, 161
- APIs, 168
  - authorization, 170
  - protection, 169
  - security, 170
- architecture, 161
- authorization, 164, 166
  - AAT tokens, 165
  - HTTP Authorization header, 166
  - permission-ticket identifier, 167
  - requesting party, 168
  - requesting party
    - token (RPT), 165
  - 401 response, 165
- ProtectServe, 155
  - authorization manager (AM), 155–156
  - consumer access token, 158
  - OAuth credentials, 159–160
401 response, 157
service provider (SP), 155
resource protection
  access, 168
centralized authorization server, 162
dynamic client-registration, 162
PAT token, 163

W, X, Y, Z
Web resource authorization profiles (WRAP), 73
  autonomous client profiles, 91
    Assertion profile, 92
    client account profile, 92
    Password profile, 92
  grant types, 95
    authorization code, 96
    client credentials, 101
    implicit code, 98
    resource owner, 100
  internet identity workshop (IIW), 91
  protected resource, 95
token types, 95, 102
  Bearer token profile, 102
  MAC token profile, 102
  user delegation profiles, 91
    Rich APP profile, 94
    username and password profile, 93
    Web APP profile, 93

WSO2 Identity Server, 178