Index

A

access control, 21, 23, 67-72, 89-100
- Extensible Access Control Markup (XACML) and, 70, 72
- fine-grained (entitlement management) and, 71-72, **71**
- identities and, 68
- identity stores (multiple) and, 70
- Lightweight Directory Access Protocol (LDAP) and, 70
- policy administration points (PAPs) in, 72
- policy decision points (PDPs) in, 71-72, 107, **107**
- policy enforcement points (PEPs) in, 71-72, **71**, 106-107, **107**
- privacy and, 13
- provisioning and, 75
- regulatory oversight/compliance and, 117
- Role-Based (RBAC), 89
- roles in, 89-100. *See also* roles
- Security Assertion Markup Language (SAML) and, 70
- single sign-on (SSO), 68-70
- user accounts, 23

Active Directory, 24, 54, 76, 80, 102

agents, for single sign-on (SSO), 106, **107**

aggregated data, privacy and, 13

anonymity, privacy and, 13

assurance levels, authentication and, 65

attributes of identity, 11, 28-29, 196

auditing and reporting, 139
- best practices for, 121-126, **124**, **125**, 125*t*, **126**, 126*t*
- federated authentication systems and, 126-127
- links analysis and, 123-126, **124**, **125**, 125*t*, **126**, 126*t*
- pattern reporting in, 118-120
- pattern-based, 117-118
- regulatory oversight/compliance and, 116

auEduPerson, 114

Australia, national identity card scheme in, 3

Australian Access Federation (AAF), 114

authentication, 2, 10, 57-67
- access control and, 67-72. *See also* access control
- assurance levels for, 65
- authorization vs., 22, 58-59, **59**
- biometrics in, 61, 63
- challenge response systems in, 60-61
- choosing correct methodology for, 63-64
- combining methods of, 61
- definition of, 57-58
- digital certificates and, 15-16, 61, 196-197
- evidence of identity (EoI) process in, 15-16, 59
- Extensible Access Control Markup Language (XACML) and, 197
- federated, 109-114, **111**, 139, 197. *See also* federated authentication

NOTE: Boldface indicates illustrations; t indicates a table.

authentication, *continued*
- fine-grained access control and, 7, 197
- identification and, 59-60
- importance of, 57
- Integrated Windows Authentication (IWA) and, 105, 139
- integration/unification of, 139
- levels of, 4, 64-65, **64**
- methods of, 59-64
- one-factor, 61-62
- passwords and, 59-62
- protection of data through, 60-61
- public key infrastructure (PKI) and, 197, 203, 203-204*t*
- registration assurance levels for, 66-67, 66*t*, **67**
- repudiation and, 60
- risk levels vs. level of, 65, 65*t*
- roles/RBAC and, 98
- Security Assertion Markup Language (SAML) and, 197
- shared secret methodology in, 61-62
- single sign-on (SSO) and, Windows systems, 105, 108
- single-level, 4
- standards for, 196-197
- three-factor, 4, 63
- trusted third parties and, 14-16
- two-factor, 4, 62-63
- validation and, 58-59, **59**

authentication directory identity store, 24

authoritative sources of identity, 47-48

authorization, 22
- authentication and vs., 58-59, **59**
- authoritative sources and, 47-48
- parallel, 87
- provisioning and, 87
- sequential, 87

authorization database identity store, 24

B

best-of-breed vs. vendor-suite solutions, 133

biometrics, 4, 61, 63

breaches of security, 1-2, 5-6

browsers and SSO, 102

budgeting for identity management, 141-142

Business at the Speed of Thought (Gates), 57

business needs evaluation, 131

business policy, regulatory oversight/compliance and, 120-121. *See also* policies, policy enforcement

C

case study, 179-193

Central Authentication Service (CAS), in single sign-on (SSO), 104, 104*t*

central directory server, 25-26, **25**

central directories, 52-55

certificate authority (CA), 150-158, **159**, 172, 205

certificate policy document, 156

certificate practice statement (CPS), 153-154, 157

certificate revocation list (CRL), 155-156, 161, 164*t*

certificate server, PKI and, 150

certificate. *See* digital certificates

challenge response systems, 60-61

cleansing. *See* data cleansing

client-side PKI, 153

Code Division Multiple Access (CDMA), smartcards and, 168

collator, smartcards and, 173

collection of data vs. privacy, 12

“collectors” and roles, 119

compliance. *See* regulatory oversight/compliance

components of a person’s identity, 10-11

confidentiality, 2

consent for use of data, privacy and, 14

contact smartcards, 175

cookies, in single sign-on (SSO) and, 105-106

corporate structure and governance model, 142-143

cost/efficiency, roles/RBAC and, 30, 92, 95

cross-domain single sign-on (SSO), 108

CRUD approach, 23

cryptography standards, 203, 203-204*t*

cryptographic message syntax standard, 203*t*

D

data cleansing, 121-126, **124**, **125**, 125*t*, **126**, 126*t*
- cost vs. accuracy curve for, 145, **145**

data integrity, 2
data security. *See* security
databases vs. directories, 37-38, 38*t*, 48-49
DB2, 24
de-provisioning, 48, 75-76. *See also* provisioning
  actions associated with, 76
  "collectors" and, 119
  directories and, 48
  roles and, 84
delegated administration, 32
delta updates, in provisioning, 86
Diffie-Hellman key agreement standard, 203*t*
digital certificates, 15-16, 61, 196-197. *See also* public key infrastructure (PKI)
  certificate authority (CA) in, 150, 151, 153, 154, 156, 158, **159**, 205
  certificate policy document for, 156
  certificate practice statement (CPS) for, 153-154, 157
  certificate production in, in-house vs. third-party, 161-162, 162*t*
  certificate revocation list (CRL) for, 155-156, 161, 164*t*, 205
  certificate server in, 159
  encryption and, 161
  extensions for, X.509 standard, 206
  hardware security modules (HSM) in, 154-155
  issuer name for, 205
  issues related to, 161
  issuing process in, 153-155, **154**
  key generation for, 160, 162-163, 163*t*
  Lightweight Directory Access Protocol (LDAP) and, 159
  management of, 160
  OCSP responder for, 156, 161, 164*t*
  public key certificates in, 151
  public key infrastructure (PKI) and, 197
  registration authority (RA) in, 153, 154
  relative distinguished name (RDN) and, 151
  revocation process for, 155-156, 161, 163-164, 164*t*
  serial number of, 205
  signature algorithm identifier for, 205
  soft vs. hard, 151-152
  subject name for, 205-206
  subject public key information in, 206
  token storage for, 164-165, 165*t*
  validity period of, 205
  version of, 205
  X.500 standard for, 206
  X.509 standard for, 156, 157-158, 196-197, 205-206
Digital Signature Algorithm (DSA), 207
digital signatures, PKI and, 148
directories, 37-56, 130, 138
  access protocols for, 196
  agility of, 37
  attributes in, 196
  authoritative sources for, 47-48
  central directory configuration for, 52-55
  configuration for, 52-55
  databases vs., 37-38, 38*t*
  de-provisioning of, 48
  design of, 48-49
  Directory Access Protocol (DAP) and, 43, 196
  directory information tree (DIT) for, 39, 46, 195
  distinguished names in, 41
  distributed configuration for, 52-55
  dynamic abilities of, 37
  groups within, 54
  inetOrgPerson schema for, 39, 196
  issues associated with, 46-47
  legacy systems and, 49
  Lightweight Directory Access Protocol (LDAP) and, 43, 44-45, 47, 50, 196
  logical topology for, 53-54, **54**
  meta-, 51
  names within, 39, 41, **42**
  namespace for, 39, **39**, 42-43
  object classes in, 39-40
  organizational units (OUs) in, 41, 42, 43
  physical topology of, 54-55
  provisioning of, 48
  relative distinguished names (RDNs) in, 41, **42**
  replication in, 52-53
  requirements of, 37
  Resource Access Control Facility (RACF), 50
  schema for, 38-41
  searches in, allowing for fuzzy/soundex, 46

NOTE: Boldface indicates illustrations; t indicates a table.

directories, *continued*
security and, 37
speed of access/response in, 37
standards for, 195-196
synchronization in, 52-53
views of organization through, 45, **45**
virtual directories and, 49-51
virtual, 138-139
X.500 standard and, 40-41, 40*t*, 43, **44**, 195-196
Directory Access Protocol (DAP), 43, 196
directory information tree (DIT), 39, 46, 195
disclosure of data vs. privacy, 13
distinguished names, 41
distributed directories, 52-55
distributed repositories, 26-27, **26**
DIT. *See* directory information tree (DIT)
diversified provisioning models, 78-81, **79**, **80**
domains of identity, 11
Domino, 102
duplication/errors in identity data, 18

E

eDirectory, 24, 102
eduPerson, 196
efficiency. *See* cost/efficiency
electronic forms packages, for provisioning, 84-85
electronic funds transfer point of sale (EFTPOS) terminals, 168
Electronic Health Signature Authority (Australia), 157
electronic identity (eID) schemes, smartcards in, 167, 169, 170
Elliptic Curve DSA (ECDSA), 207
encryption and PKI, 148, 161
Enron, 115
Enterprise Resource Planning (ERP) systems vs. roles/RBAC, 95
enterprise single sign-on (ESSO), 102-105, 138. *See also* single sign-on (SSO)
entitlement management, 71-72. *See also* fine-grained authentication
errors in identity data, 18
Europay, Mastercard, Visa (EMV) standards, 168
evidence of identity (EoI) checks, 15-16, 59, 171-172
exercises/university case study, 179-193
existing IT environment evaluation, 131-132
extended-certificate syntax standard, 203*t*
Extensible Access Control Markup Language (XACML), 70, 72, 197

F

facial recognition, 4, 61. *See also* biometrics
federated authentication, 109-114, **111**, 139, 197
auditing of systems using, 126-127
identity providers (IdPs) in, 109-111, 127
inetOrgPerson schema for, 114
Lightweight Directory Access Protocol (LDAP) in, 113-114
pitfalls of, 113-114
Security Assertion Markup Language (SAML) and, 113
service providers (SPs) in, 109-111
Shibboleth credentialing in, 113
Where Are You From (WAYF) server systems for, 112-113, **112**
financial sector
and increasing regulatory issues, 115
and smartcard use, 168
fine-grained authentication (entitlement management), 7, 71-72, **71**, 197
fingerprints, 4, 61. *See also* biometrics
Firefox, 102
forms, for provisioning, 84-85
future developments in identity management, 4-7
fuzzy searches, 46

G

gap analysis, 132
Gates, Bill, 57
generic attributes of identity, 10-11
Global Platform alliance and smartcards, 169, 171
Global System for Mobile Communications (GSM) and smartcards, 168
governance, 115-116, 142-143
governance, risk, and compliance (GRC), 115-128. *See also* regulatory oversight/compliance
groups, 54, 118

GroupWise, 76
Guilloche patterns on smartcards, 174

H

hackers, 1
hard certs, 151-152
hardware security module (HSM), 154-155, 172-173
Health Insurance Portability and Accountability Act (HIPAA), 115
HR-centric vs. diversified provisioning models, 78-81, **79**, **80**
HTTP and single sign-on (SSO), 105, 106, 107

I

IBM, 143
IBM i systems, 69
identification papers/cards, 2-3
identifiers, 13-14
identity, 9-20
  access control and, 68
  attributes of, 11, 28-29
  authentication of, 10
  authoritative sources of, 47-48
  components of, 10-11
  data cleansing and, 121-126, **124**, **125**, 125*t*, **126**, 126*t*, 145
  defining, 9-10, 11
  domains of, 11
  duplication/errors in data for, 18
  generic attributes in, 10-11
  identity stores and, 27-28
  multiple, within one environment, 17-18
  privacy and, 11-16
  registration assurance levels for, 66-67, 66*t*, **67**
  roles and, 16-17
  source of truth for, 47-48
  specific attributes in, 10-11
  trust in establishing, 10
  user accounts and, 22-23
  X.500 standard and, 40-41, 40*t*, 195-196
identity management, 21-35
  access control in, 21, 23
  applications of, 5
  authentication in, 22
  authorization in, 22
  automated processes in, 3-4
  cleansing, data cleansing for, 121-126, **124**, **125**, 125*t*, **126**, 126*t*, 145
  CRUD approach in, 23
  definition of, 2
  delegated administration and, 31-32
  duplication and errors in, 18
  federated authentication and, 109
  future developments in, 4-7
  government control of citizens and, 4-5
  history and development of, 2-3
  identity stores in, 21-35. *See also* identity stores
  implementation of, 129-146. *See also* implementation and roadmap
  levels of identity data needed in, 6
  links analysis and, 123-126, **124**, **125**, 125*t*, **126**, 126*t*
  multiple identities for one person and, 17-18
  pitfalls of, 5-6
  regulatory oversight/compliance and importance of, 23, 116
  self-service approach to, 5, 31-32
  separation of duties (SoD) policies and, 21, 93, 127, 120-121
  state of the industry in, 3-4
  user accounts and, 22-23
identity providers (IdPs), for federated authentication, 109-111, 127
identity stores, 21-35, 131-132
  access control and, 70
  attributes of identity in, 28-29
  authentication directory type of, 24
  authorization database type of, 24
  central directory server for, 25-26, **25**
  definition of, 23-24
  delegated administration for, 31-32
  directory provisioning in, 29-30
  distributed repositories for, 26-27, **26**
  identities in, 27-28
  joins and, 26
  legacy applications and, 25

identity stores, *continued*
  Lightweight Directory Access Protocol (LDAP) and, 25
  multiple, 24-30, 70
  multiple, management strategies for, 27-30
  provisioning of, 29, 75-88. *See also* provisioning
  role management in, 30, **31**
  role modeling for, 32
  types of, 24
  virtual directories and, 26-27
implementation and roadmap, 129-146
  budget management for, 141-142
  business needs evaluation for, 131
  challenges to, 141-145
  components that may be required in, 138-139
  corporate structure and governance model for, 142-143
  data cleansing cost vs. accuracy curve in, 145, **145**
  directories in, 130
  existing IT environment evaluation for, 131-132
  gap analysis in, 132
  identity stores in, 131-132
  physical infrastructure/implementation in, 135-136
  political landscape and, dealing with, 140-141
  pre-implementation tasks in, 130-135
  project management for, 145
  project structure for, typical, 136-138
  request for proposal (RFP) process for 133-135
  risk analysis for, 132-133, 137-138, 137*t*
  roadmap creation for, 133, 135
  sample roadmap for, 138-140, **139**
  skilled resources needed for, 142
  sponsor and stakeholders in, 131, 140-141
  technical solution evaluation for, 132
  vendor churn and, 143
  vendor strategies used in, 143-145
  vendor-suite vs. best-of-breed solutions in, 133
implementing a PKI certificate system, 161-165
iNetOrg Person (Microsoft), 196
inetOrgPerson schema, 39, 114, 196
Infocard, 16
integrated authentication, 139
Integrated Windows Authentication (IWA), 105
Internet Explorer, 102
Internet Information Services (IIS) for SSO, 108
Internet Taskforce RFC 2798, 39
Internet, business use of/connection to, 57
iris scans, 4, 61. *See also* biometrics
ISO 24727 standard, 169, 174
ISO 7816 standard, 169, 174
IT controls, regulatory oversight/compliance and, 120-121
IT environment evaluation, 131-132

J

Java 2 Platform, Enterprise Edition (J2EE) for SSO, 108
Java Authentication and Authorization Service (JAAS) for SSO, 104, 104*t*
Java Card, 169, 174
joins, 26

K

Kerberos, 103-104, 104*t*
key generation, in PKI, 160, 162-163, 163*t*
key lengths, PKI, 207
key pairs, 148

L

legacy systems, 25, 49
levels of authentication, 64-65, **64**
Lightweight Directory Access Protocol (LDAP), 144
  access control and, 70
  digital certificates and, 159
  directories and, 43, 44-45, 47, 50, 196
  federated authentication and, 113-114
  identity stores and, 25
  PKI and, 159
  Resource Access Control Facility (RACF) directories and, 50
  virtual directories and, 50
links analysis, 123-126, **124**, **125**, 125*t*, **126**, 126*t*
locking a smartcard, 176
logical directory topology, 53-54, **54**
Lotus Notes, 50, 76, 102

M

managing identity. *See* identity management
mapping roles, 82-83, **82**, 90-91, 90-91*t*
meta-directories, 51
micro-printing on smartcards, 174
Microsoft, 196
  Active Directory, 24
  Exchange Server, 69
  Exchange, 76, 105
  Infocard, 16
  Outlook, 105
  SharePoint, 87
  Windows. *See* Windows
mobile phones and smartcards, 168
modeling roles, 32
MOTO rules, 60
multiple identities for one person, 17-18
multiple identity stores, 24-30. *See also* identity stores
MVS, 24

N

names, 39, 41, **42**
  directory, 39, 41, **42**
  distinguished, 41
  relative distinguished (RDNs), 41, **42**
namespace, 39, **39**, 42-43, **44**
national identification papers/cards, 2-3
National Institute of Standards and Technology (NIST), 207
.NET, 24
Netscape, 196
non-repudiation, 2
Novell, 18, 76
  eDirectory, 24, 102
  GroupWise, 76

O

object classes in directory, 39-40
OCSP responder, 156, 161, 164*t*
Omada Identity Manager, 89
OpenSSO, 104, 104*t*
Oracle, 24, 50, 69, 76, 143, 144
  Federation Server, 144
  Internet Directory, 144
organizational units (OUs), 41, 42, 43
organizationalPerson, 196
orphan accounts, 118

P

parallel authorization, 87
password-based cryptography standard, 203*t*
passwords, 53, 59-62
pattern reporting, 118-120
pattern-based auditing, 117-118
physical infrastructure/implementation, 135-136
PIN numbers, 4, 62, 63, 171
pitfalls of identity management systems, 5-6
policies, policy enforcement
  regulatory oversight/compliance and, 120-121
  restriction table sample for, 120, 121*t*
  single sign-on (SSO) and, 108-109
policy administration points (PAPs), in access control, 72
policy decision points (PDPs), 71-72, 107, **107**
policy enforcement points (PEPs), 71-72, 106-107, **107**
printing a smartcard, 173, **173**
privacy, 11-16. *See also* security
  access and transparency of data vs, 13
  aggregation and anonymity in, 13
  breaches of, 1-2, 5-6
  collection of data and, 12
  consent for use of data and, 14
  digital certificates and, 15-16
  identifiers and, 13
  increasing protection of, 12
  PKI and, 149-150
  quality of data and, 13
  regulatory oversight and importance of, 23
  rules for protecting, 12-14
  security and, 13
  sharing data and, 14
  smartcards and, 170-171
  trust vs., 11
  trusted third parties and, 14-16
  use and disclosure of data vs, 13
private key, 148
private-key information syntax standard, 203*t*

productivity and roles/RBAC, 92, 95
project management in implementation, 145
provisioning, 29, 75-88
  access control/access rights and, 75
  Active Directory and, 80
  authorization in, sequential and parallel, 87
  automation of, 29, 84-87
  business system issues to confront in, 78-81
  "collectors" and, 119
  de-, 48, 75. *See* de-provisioning
  definition of, 75
  delta updates to, 86
  directories and, 48
  directory level, 29-30
  electronic forms packages for, 84-85
  HR-centric vs. diversified models for, 78-81, **79**, **80**
  minimal data entry criterion for, 76
  public key infrastructure (PKI) and, 85
  robustness of, marks of, 76-78, 76
  role mapping in, 82-83, **82**
  roles/RBAC and, 81-84, 98
  security and, 78-79
  self- self-service approach to, 77
  signatures in, 85
  synchronization, data synchronization and, 86-87
  workflow engine for, 81, 85-86
  zero-day start goal for, 78
proxies in single sign-on (SSO), 106, **107**
public key, 148
public key certificates in, 151
public key cryptography standards, 203, 203-204*t*
public key infrastructure (PKI), public key infrastructure (PKI), 148-166, **149**, 197. *See also* digital certificates
  certificate authority (CA) in, 150, 151, 153, 154, 156, 158, **159**
  certificate management and, 160
  certificate policy document for, 156
  certificate practice statement (CPS) for, 153-154, 157
  certificate production in, in-house vs. third-party, 161-162, 162*t*
  certificate revocation list (CRL) for, 155-156, 161, 164*t*
  certificate server in, 150, 159
  client-side, 153
  components of, 153-159
  cryptography standards for, 203, 203-204*t*
  digital signatures and, 148
  encryption and, 148, 161
  hardware security modules (HSM) in, 154-155
  implementation considerations for, 161-165
  important uses of, 149-150, 152-153
  issues related to certificates and, 161
  issuing process in, 153-155, **154**
  key generation for, 160, 162-163, 163*t*
  key lengths in, 207
  key pairs in, 148
  Lightweight Directory Access Protocol (LDAP) and, 159
  OCSP responder for, 156, 161, 164*t*
  privacy and, 149-150
  private key in, 148
  process of using, 148-149, **149**, 150-152, **150**
  provisioning and, 85
  public key certificates in, 151
  public key in, 148
  registration authority (RA) in, 153, 154
  relative distinguished name (RDN) and, 151
  revocation process for, 155-156, 161, 163-164, 164*t*
  security and, 149-150
  server-side, 152-153
  smartcards and, 148, 151, 174
  soft vs. hard certs in, 151-152
  storage device production for, 165, 165*t*
  strength of certificate in, 151
  terminology of, 151-152
  token storage for, 164-165, 165*t*
  USB devices and, 151
  X.509 standard for, 156, 157-158

Q

quality of data vs. privacy, 13

R

registration assurance levels, authentication and, 66-67, 66*t*, **67**

registration authority (RA), 153, 154
registration system for smartcards, 171-172
regulatory oversight/compliance, 23, 115-128
  access control and, 117
  auditing and reporting in, 116
  business policies and, 120-121
  "collectors," 119
  compliance defined for, 116
  data cleansing and, best practices for, 121-126, **124**, **125**, 125*t*, **126**, 126*t*
  federated authentication auditing and, 126-127
  financial sector and, 115
  governance and, 115-116
  groups in, 118
  Health Insurance Portability and Accountability Act (HIPAA) and, 115
  identity management's role in, 116
  increasing levels of, 115
  IT controls and, 120-121
  links analysis and, 123-126, **124**, **125**, 125*t*, **126**, 126*t*
  orphan accounts and, 118
  pattern reporting in, 118-120
  pattern-based auditing in, 117-118
  risk management and, 116
  roles and role management for, 30, 95, 118
  Sarbanes-Oxley Act and, 115
  separation of duties (SoD) policies and, 120-121, 127
relative distinguished name (RDN), 41, **42**, 151
replay attacks vs. SSO, 106
replication, 52-53
repository, distributed, 26-27, **26**
repudiation, 2, 60
request for proposal (RFP) process 133-135
Resource Access Control Facility (RACF), 50, 102, 118
restriction table sample, 120, 121*t*
reverse proxy server for SSO, 106
revocation process, digital certificates and PKI, 155-156, 161, 163-164, 164*t*
risk analysis, 132-133, 137-138, 137*t*
risk management, 116
  authentication and levels, 65, 65*t*
  impact, mitigation, risk owner in, 137
  implementation and, 132-133, 137-138, 137*t*
  registration assurance levels for, 66-67, 66*t*, **67**
  residual risk in, 138
  risk level matrix in, 137-138, 137*t*
  roles use and, 30
  severity, likelihood, and level in, 137
roadmap. *See* implementation and roadmap
role-based access control. *See* roles and role-based access control (RBAC)
roles and role-based access control (RBAC), 16-17, 89-100
  access control using, 89-100
  access rights and, 98
  authentication and, 98
  basic process of, 90
  benefits of, in provisioning, 83-84
  bottom up vs. top down planning for use of, 17
  business process improvement using, 95
  change, speed of response to, 94
  "collectors" and, 119
  cost savings of, 30
  data cleansing and, 121-126, **124**, **125**, 125*t*, **126**, 126*t*, 145
  de-provisioning and, 84
  defining, 97
  delegated administration of, 31-32
  discovery of, 97-98
  efficiency and, 92, 95
  Enterprise Resource Planning (ERP) systems vs., 95
  exceptions for, 97
  heterogeneous system management through, 94
  identity and, 16-17
  identity stores and, 30, **31**
  implementation of, 95-97
  importance of, 92
  links analysis and, 123-126, **124**, **125**, 125*t*, **126**, 126*t*
  management of, 30, **31**
  mapping of, 82-83, **82**, 90-91, 90-91*t*
  modeling of, 32
  multiple identities for one person and, 17-18
  number of, 96
  overlapping, 123-126
  pattern reporting in, 118-120

roles and role-based access control *continued*
pattern-based auditing of, 118
planning for use of, bottom up vs. top down, 17
productivity and, 92
provisioning and, 81-84, 98
regulatory oversight/compliance and, 30, 95, 118
Resource Access Control Facility (RACF), 118
restriction table sample for, 120, 121*t*
risk management and, 30
Role-Based Access Control (RBAC) and, 89
SAP-defined, 118
scalability of system and, 94-95
security and, 93, 94, 97-98
separation of duties (SoD) policies and, 21, 93, 120-121, 127
RSA cryptography standard, 203*t*, 207

S

SAP, 18, 89, 118
Sarbanes-Oxley Act (SOX), 23, 115
schema for directory, 38-41
searching a directory, 46
Secure Sockets Layer (SSL) and SSO, 106, 108
security, 1. *See also* privacy
authentication and, 60-61
breaches of, 1-2, 5-6
digital certificates and, 15-16
directories and, 37
Extensible Access Control Markup (XACML) and, 70, 72
hardware security modules (HSM) in, 154-155
PKI and, 149-150
privacy and, 13
provisioning and, 78-79
regulatory oversight and importance of, 23
roles/RBAC and, 93, 94, 97-98
Secure Sockets Layer (SSL) and, 106, 108
Security Assertion Markup Language (SAML) and, 70, 104, 104*t*, 108, 113, 197
Security Assertion Markup Language (SAML), 70, 197
federated authentication and, 113
single sign-on (SSO) and, 104, 104*t*, 108
selected attribute types standard, 203*t*
self-service approach to identity management, 5, 31-32
self-service approach to provisioning, 77
separation of duties (SoD) policies, 21, 93, 120-121, 127
sequential authorization, 87
server-side PKI, 152-153
servers
central directory, 25-26, **25**
certificate, in PKI systems, 150, 159
PKI on, 152-153
reverse proxy, 106
Where Are You From (WAYF), for federated authentication, 112-113, **112**
service providers (SPs), federated authentication and, 109-111
session cookies, SSO, 106
session time-outs, SSO, 106
sessions, SSO, 103-104
SHA-1/SHA-2, 207
shared data and privacy, 14
shared secret methodology in authentication, 61-62
SharePoint, 87, 102
Shibboleth credentialing, 113
signatures, 85, 148. *See also* digital signatures
single sign-off, 104
single sign-on (SSO), 68-70, 101-109
agents in, 106, **107**
Central Authentication Service (CAS) and, 104, 104*t*
challenges of, 101-102
cookies and, 105-106
cross-domain, 108
enterprise (ESSO), 68-70, 102-105, 138
HTTP and, 105, 106, 107
Internet Information Services (IIS) and, 108
Java 2 Platform, Enterprise Edition (J2EE) and, 108
Java Authentication and Authorization Service (JAAS) for, 104, 104*t*
Kerberos and, 103-104, 104*t*
need for, 101
OpenSSO for, 104, 104*t*
policies and policy enforcement for, 108-109
policy decision points (PDPs) in, 107, **107**

policy enforcement points (PEPs) in, 106-107, **107**
proxies in, 106, **107**
replay attacks vs., 106
reverse proxy server in, 106
Secure Sockets Layer (SSL) and, 106, 108
Security Assertion Markup Language (SAML) and, 104, 104*t*, 108
session cookies in, 106
session time-outs and, 106
sessions in, 103-104, 105-106
single sign-off and, 104
standards development for, 104, 104*t*
tokens/smartcards and, 106
Trusted Platform Modules (TPMs) and, 106
virtual private networks (VPNs) and, 108
Web browser use of, 102
Web, 68-70, 105-109, **107**, 138
Windows and, integrated authentication (IWA) for, 105, 108

skilled resources needed for implementation, 142
Smartcard Management System (SCMS), 172
smartcards, 151, 167-177
card keys vs. certificate keys in, 172
certificate authority (CA) for, 172
Code Division Multiple Access (CDMA) and, 168
collator for, 173
components of system using, 171
contact vs. wireless cards in, 175
data structure of, 174-175
deployment issues for, 171-176
electronic funds transfer point of sale (EFTPOS) terminals for, 168
electronic identity (eID) schemes using, 167, 169, 170
Europay, Mastercard, Visa (EMV) standards for, 168
evidence of identity (EoI) process for, 171-172
financial sector use of, 168
Global Platform alliance and, 169, 171
Global System for Mobile Communications (GSM) and, 168
hardware security module (HSM) for, 172-173
history of, 166-167
identification sector use of, 169
interoperability issues for, 169-170
ISO 24727 and, 169, 174
ISO 7816 standard for, 169, 174
issuance of, 176
Java Card and, 169, 174
key generation for, 160, 162-163, 163*t*
lifecycle of, 175-176
locking of, 176
manufacturing of, 175
mobile phone sector use of, 168
personalization of, 175-176
physical layout and design of, 173-174
PKI and, 148
printing of, printers for, 173, **173**
privacy issues and, 170-171
public key infrastructure (PKI) and, 174
registration system for, 171-172
single sign-on (SSO) and, 106
Smartcard Management System (SCMS) for, 172
standards for, 169, 174
storage device production for, 165, 165*t*
Subscriber Identity Module (SIM) cards and, 168
termination of, 176
ticketing sector use of, 168-169
token storage in, 164-165, 165*t*
"touch-and-go" technology and, 169

soft certs, 151-152
soundex searches, 46
source of truth, 47-48
specific attributes of identity, 10-11
SQL, 24
stakeholders in implementing identity management systems, 131, 140-141
standards, 195-197
authentication, 196-197
digital certificates and, 196-197
Directory Access Protocol (DAP) and, 196
directory, 195-196
Europay, Mastercard, Visa (EMV), 168
Extensible Access Control Markup Language (XACML) and, 197
fine-grained access control, 197

standards, *continued*
- Lightweight Directory Access Protocol (LDAP) and, 196
- public key cryptography, 203, 203-204*t*
- Security Assertion Markup Language (SAML) and, 197
- single sign-on (SSO) and, 104, 104*t*
- smartcards and, 169, 174

storage device production, PKI, 165, 165*t*
Subscriber Identity Module (SIM) cards, 168
Sun Identity Manager, 144
SunONE directory, 24, 76, 144
synchronization
- directories and, 52-53
- provisioning and, 86-87

T

technical solution evaluation, 132
terminating a smartcard, 176
Thawte, 15
ticketing sector use of smartcards, 168-169
token storage, PKI, 164-165, 165*t*
"touch-and-go" technology and smartcards, 169
transparency of data, 13, 23
trust, 10, 11, 14-16
trusted identifiers, 14
Trusted Platform Modules (TPMs), 106
trusted third parties and, 14-16

U

unified authentication, 139
University case study, 179-193
USB devices
- key generation for, 160, 162-163, 163*t*
- PKI and, 151
- storage device production for, 165, 165*t*
- token storage in, 164-165, 165*t*

use of data vs. privacy, 13
user accounts, 22-23

V

validation, 33, 58-59, **59**
- authentication and vs., 58-59, **59**

vendors, in implementation and management, 143-145
vendor-suite vs. best-of-breed solutions, 133
VeriSign, 15
virtual directories, 26-27, 49-51, 138-139
- identity stores and, 26-27
- legacy systems and, 49
- Lightweight Directory Access Protocol (LDAP) and, 50
- limitations of, 27
- meta-directories vs., 51

virtual private networks (VPNs) and SSO, 108

W

Web browsers and SSO, 102
Web SSO, 105-109, **107**, 138. *See also* single sign-on
Where Are You From (WAYF) server systems, 112-113, **112**
Windows and SSO, integrated authentication for, 105, 108
wireless smartcards, 175
workflow engine, in provisioning, 81, 85-86
WorldCom, 115

X

X.500 standard, 40-41, 40*t*, 43**, 44**, 195-196, 206
X.509 standard, 15, 156, 157-158, 196-197, 205-206

Z

zero-day start goal for provisioning, 78