Inhaltsverzeichnis

Vorwort ..... **VII**

1 Elemente zur Berechtigungssteuerung **1**

1.1 Berechtigung 1

1.2 Rolle 10

1.2.1 Business-Rolle 10

1.2.2 Technische Rolle 12

1.3 Attribut 12

1.4 Gruppe 14

1.5 Arbeitsplatzprofil 15

1.6 Workset 15

1.7 Profil 16

1.8 Sammelprofil 19

2 Identitätsmanagement **21**

2.1 Der Identitätsbegriff 21

2.2 Identitätsarten 23

2.3 Identitätsträger 25

2.4 Identifizierung einer Identität 29

2.4.1 Identifizierung über Namen 29

2.4.2 Identifizierung mit abstrakten Bezeichnern 31

2.4.3 Fazit 33

2.5 Schutz der Privatheit 33

2.5.1 Identitätsgefahren 34

2.5.2 Identitätsmanagement 35

Bibliografische Informationen
http://d-nb.info/999240773

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

3 Rollenkonzept 41
3.1 Motivation für die Verwendung von Rollen 41
3.2 Rollenfindung und Rollenbildung 45
3.2.1 Auswertung von Dokumentationen 45
3.2.2 Aufnahme der Tätigkeiten 47
3.3 Rollenhierarchie 55
3.3.1 Rollenbeziehungen 55
3.3.2 Vererbung von Rollen 59
3.4 Anwendungsbeispiel der Rollenhierarchie 60
3.5 Rollenmodelle 67
3.5.1 Multiple Role Model 67
3.5.2 Single Role Model 68

4 Role Based Access Control 69
4.1 Core RBAC 70
4.1.1 Referenzmodell 70
4.1.2 Funktionale Spezifikation 71
4.2 Hierarchical RBAC 75
4.2.1 Referenzmodell 75
4.2.2 Funktionale Spezifikation für das General Hierarchical RBAC 76
4.3 Constrained RBAC 77

5 Berechtigungssteuerung 81
5.1 Die zwei Seiten der Berechtigungsthematik 81
5.1.1 Seite der Identitäten 81
5.1.2 Seite der Ressourcen 82
5.2 Quelldaten 84
5.2.1 Personaldaten 85
5.2.2 Organisationsdaten 87
5.2.3 Systemdaten 87
5.2.4 Applikationsdaten 88

5.3 Rollenbasierte Berechtigungssteuerung ... 88
5.4 Attributsbasierte Berechtigungssteuerung ... 93
5.5 Gruppenbasierte Berechtigungssteuerung ... 95
5.6 Kombinierte Berechtigungssteuerung ... 96
5.7 Granularität der Berechtigungssteuerung ... 104
5.8 Berechtigungsmodelle ... 109

6 Provisioning ... 115
6.1 User und Ressource Provisioning ... 116
6.1.1 User Provisioning ... 116
6.1.1. 120
6.1.2 Ressource-Provisioning ... 120
6.2 Server Provisioning ... 123
6.3 Service Provisioning ... 124
6.4 Mobile Subscriber Provisioning ... 126
6.5 Mobile Content Provisioning ... 126

7 Zugriffskontrolle über Authentifizierung ... 127
7.1 UserID und Passwort ... 128
7.2 Splitted Password ... 132
7.3 Challenge Response ... 133
7.4 Ticket-Systeme ... 136
7.5 Authentifizierung nach Needham und Schroeder ... 136
7.5.1 Kerberos ... 137
7.5.2 SESAME ... 140
7.5.3 DCE – Distributed Computer Environment ... 141
7.6 Authentifizierung über Token ... 141
7.6.1 Synchrone Token-Erstellung ... 142
7.6.2 Asynchrone Token-Erstellung ... 143
7.6.3 Duale Authentifizierung ... 143

7.7 Digitale Zertifikate und Signaturen ... 144
7.7.1 Digitale Zertifikate ... 144
7.7.2 Digitale Signatur ... 146
7.8 Biometrie ... 148
7.8.1 Biometrie in der praktischen Anwendung ... 149
7.9 PKI – Public Key Infrastructure ... 152
7.10 Anforderungen an Authentifizierungsdienste ... 154

8 Zugriffskontrolle über Autorisierung ... 159
8.1 Identitätsbezogene Zugriffskontrolle ... 162
8.2 Ressourcenorientierte Zugriffskontrolle ... 162
8.3 Klassifizierungsorientiert am Objekt und Subjekt (Macintosh) – Sensitivity Labels 164
8.4 Rollenbasierte Zugriffskontrolle ... 164
8.5 Zugriffskontrolltechnologien ... 165
8.5.1 Rollenbasierte Zugriffskontrolle ... 165
8.5.2 Regelbasierte Zugriffskontrolle ... 166
8.5.3 Schnittstellen mit eingeschränkten Rechten ... 166
8.5.4 Zugriffskontrollmatrix ... 167
8.5.5 Autorisierungstabellen ... 167
8.5.6 Zugriffskontrolllisten – ACL – Access Control List ... 168
8.5.7 Inhaltsabhängige Zugriffskontrolle ... 168
8.6 Verwaltung der Zugriffskontrolle ... 168
8.6.1 Zentralisierte Verwaltung ... 169
8.6.2 RADIUS ... 170
8.6.3 TACACS ... 170
8.6.4 Dezentralisierte Verwaltung ... 171
8.6.5 Hybride Verwaltung ... 172
8.7 Methoden der Zugriffskontrolle ... 173

8.8 Zugriffskontrollstufen ... 173
8.8.1 Physische Kontrolle ... 173
8.8.2 Technische Kontrolle ... 174
8.8.3 Adminstrative Kontrollen ... 176

9. Single Sign On ... 181
9.1 Problematik multipler Zugänge ... 181
9.1.1 Erhöhter Helpdesk-Aufwand ... 181
9.1.2 Produktivitätsverlust durch Mehrfachanwendungen ... 182
9.1.3 Steigende Kompromittierungsgefahren ... 183
9.1.4 Sinkende Anwenderakzeptanz und sinkende Transparenz ... 183
9.2 Entwicklung von SSO ... 185
9.2.1 Passwortsynchronisierung durch den Benutzer ... 185
9.2.2 Passwortzentralisierung über die Plattform-Anmeldung ... 186
9.2.3 Passwortsynchronisierung im Backend ... 188
9.2.4 Erste echte SSO-Ansätze ... 189
9.2.5 Grenzen von SSO bei Legacy-Systemen ... 190
9.3 Aufbau eines Single Sign On-Systems ... 191
9.3.1 Repository der Zugangsdaten ... 193
9.3.2 Verwaltungssystem für die Zugangsdaten ... 195
9.3.3 Schnittstellen (APIs, Logon-Clients, Scripting Engines) ... 196
9.3.4 Strenge Authentifizierung der zentralen Anmeldung ... 199
9.3.5 Verwaltung der strengen Authentifizierung ... 200
9.4 Single-Sign-On – Die Realisierungsvarianten ... 201
9.4.1 Multifunktionale Smartcards ... 201
9.4.2 SSO über Kerberos ... 202
9.4.3 SSO über Portallösungen ... 203
9.4.4 SSO über Ticketsysteme ... 204
9.4.5 SSO über lokale Systeme ... 205
9.4.6 SSO mittels PKI ... 205
9.4.7 SSO über Firewall-Erweiterungen ... 205

9.4.8 SSO über IdM-Systeme ... 206
9.4.9 SSO über RAS-Zugänge ... 206
9.4.10 SSO für Webanwendungen mit Authentication Tokens ... 207
9.5 Technologie und Herstelleransätze für die Realisierung von SSO ... 207
9.5.1 Microsoft Passport ... 207
9.5.2 Das Liberty Alliance Project ... 208
9.5.3 Shibboleth ... 209
9.5.4 OpenID ... 209
9.5.5 Der Central Authentication Server (CAS) ... 210
9.6 Realisierung von SSO im Unternehmen ... 211
9.6.1 Vor- und Nachteile SSO ... 211
9.6.2 Kosten und Nutzen SSO ... 212
9.6.3 Auswahl eines SSO Systems ... 213
9.6.4 Wie kann man schnell SSO einführen ... 213

10 Systemnahes Berechtigungskonzept ... 215
10.1 Der Aufbau von ACF2 ... 215
10.1.1 BenutzerID-Record ... 216
10.1.2 Der UID- User Identification String ... 219
10.1.3 Die Data Set Rule ... 220
10.1.4 Die Resource Rule ... 224
10.1.5 Resumé ... 225

11 Meta Directory ... 229
11.1 Die neue Zentralität ... 229
11.2 Zentrales Repository ... 236
11.3 Aufbau eines Berechtigungssystems ... 239
11.3.1 Datenablage (Repository) ... 239
11.3.2 Zugangsschnittstelle für die Administration ... 240
11.3.3 Rule Engine ... 240
11.3.4 Provisioning-Komponente ... 240

11.3.5 Verwaltungssystem ... 243
11.3.6 Kommunikationskomponente ... 243
11.4 Grundkonzept Verzeichnisdienst ... 244
11.5 Verzeichnisstandards ... 250
11.6 Meta-Funktionalität ... 252
11.7 Meta Directory im Berechtigungsmanagement ... 254

12 Förderierte Identitäten – Identity Federation ... 259
12.1 Problem der Identitätsgrenze ... 260
12.2 Unternehmensübergreifende Kommunikation ... 261
12.2.1 Klassische Kommunikationsmittel ... 261
12.2.2 Übertragung elektronischer Informationen ... 262
12.2.3 Übertragung strukturierter elektronischer Informationen ... 262
12.3 Konzept des Service-Netzes ... 263
12.3.1 Webservices ... 263
12.3.2 Anwendungsszenarien ... 263
12.3.3 Zugriff auf externe Anwendungen ... 263
12.4 Aufbau des Protokollstacks ... 265
12.4.1 Hypertext Transfer Protrocol und Extensible Markup Language ... 265
12.4.2 SOAP – Simple Object Access Protocol ... 265
12.4.3 WSDL – Web Services Description Services ... 266
12.4.4 SAML – Security Assertion Markup Language ... 268
12.4.5 SPML – Service Provisioning Markup Language ... 270
12.4.6 DSML – Directory Service Markup Languge ... 272
12.4.7 XACML – eXtensible Access Control Markup Language ... 275
12.4.8 WS-Security ... 276
12.4.9 ID-FF – Identity Federation Framework ... 276
12.4.10 ADFS - Active Directory Federation Services ... 278
12.4.11 FIDIS – Future of Identity in the Information Society ... 278
12.4.12 Zukunftsausblick Quantenverschlüsselung ... 278

13 Rechtliche Rahmenbedingungen ... 281
13.1 SOX ... 283
13.2 KonTraG ... 285
13.3 GoBS ... 287
13.4 Datenschutzrechtliche Einflüsse ... 287
13.5 Weitere Vorschriften und Richtlinien ... 291
13.5.1 Das Internet und die GEZ ... 291
13.5.2 Neue Gesetze ... 292
13.5.3 Informations- und Risikomanagement ... 293
13.5.4 Basel II ... 294
13.5.5 MaRisk ... 295
13.5.6 Die Rechtsfolgen von Non-Compliance ... 296
13.5.7 Strafverfolgung der Emittlungsbehörden ... 297
13.5.8 Vorratsdatenspeicherung ... 297
13.5.9 Haftungsfragen ... 297
13.5.10 Identitätsdiebstahl ... 300
13.5.11 Archivierungspflichten und digitale Betriebsprüfung ... 300
13.5.12 Elektronische Rechnungen ... 301
13.5.13 Mitarbeiterkontrolle ... 302
13.5.14 Einsatz rechtssicherer Spam und Contentfilter ... 303
13.5.15 Gestaltung von Betriebsvereinbarungen ... 304
13.5.16 Abwesentheit von Mitarbeitern ... 305