

Christian Mezler-Andelberg

Identity Management – eine Einführung

Grundlagen, Technik, wirtschaftlicher Nutzen



dpunkt.verlag

Inhaltsverzeichnis

	Einleitung	1
Teil 1	Grundlagen	5
1	Warum Identity Management?	7
2	Ein Ebenenmodell für das Identity Management	13
2.1	Die Ebenen im Überblick	14
2.2	Abbildungen des Modells	17
3	Die Prozesse im Modell	19
3.1	Prozessgruppen	19
3.2	Einflussfaktoren auf die Prozesse	21
3.3	Operative Prozesse	23
3.4	Gestaltende Prozesse	24
3.5	Administrative Prozesse	25
4	Die Basisebenen im Detail	27
4.1	Ebene 1 – Personendaten	27
4.1.1	Prozesse der Ebene E1 (Personendaten)	30
4.2	Ebene 2 – Ressourcen	35
4.2.1	Prozesse von E2 (Ressourcen)	36
4.2.2	Datenklassifizierung	37
4.2.3	Berechtigungssysteme in Applikationen	39
4.3	Ebene 3 – Autorisierung	40
4.3.1	Die Prozesse von E3 (Autorisierung)	42
4.3.2	Datenzugriffsmodelle	42
4.3.3	Role-Based Access Control (RBAC)	45

4.3.4	Die Nachfolger: ABAC, RB RBAC, PBAC und Co	48
4.3.5	Ein passendes Rollenmodell entwickeln	49
4.4	Ebene 4 – Authentisierung	53
4.4.1	Prozesse von E4 (Authentisierung)	56
4.5	Die Verbindungsschichten	61
4.5.1	User Provisioning	61
4.5.2	Single Sign On (SSO)	63
5	Das gesamte Modell im Überblick	65
5.1	Die Prozesse im Modell	66
5.2	Aufgabentrennung im Modell	68
6	Federation	71
6.1	Federation im Schichtenmodell	78
7	Anwendungsmöglichkeiten des Modells	81
7.1	Das Modell als Vorgehensweise im Projekt	81
7.2	Rechtstrennung im Betrieb	83
7.3	Abbilden von Begriffen und Produkt-Suiten	85
7.4	Schnittstelle zu ITIL	85
8	Andere Darstellungsvarianten	89
8.1	Darstellung nach dem Modell der Burton Group	89
8.2	Darstellung nach Generic IAM	91
8.3	Darstellung nach Produktmerkmalen	94
Teil 2	Technik	95
9	Technische Aspekte der Ebene 1 (Personendaten)	99
9.1	Directories	101
9.2	DSML	104
9.3	Virtuelle Directories	106
9.4	Alternativen zu Directories	106
9.4.1	Relationale Datenbank als Repository	106
9.4.2	Repository im Zielsystem	107
10	Technische Aspekte der Ebene 2 (Ressourcen)	109
10.1	Anbinden von Applikationen	110
10.1.1	Wie viele Accounts braucht ein Service?	114

11	Technische Aspekte der Ebene 3 (Autorisierung)	115
11.1	XACML	117
11.1.1	Rollen und Datenfluss in XACML	118
11.1.2	Beispiel: XACML Policy	122
11.1.3	Beispiel: XACML-Anfrage	123
11.1.4	Beispiel: XACML-Antwort	125
11.1.5	RBAC mit XACML	125
11.1.6	Transportprotokolle für XACML	128
12	Technische Aspekte der Ebene 4 (Authentisierung)	131
12.1	SASL	137
12.2	TSL	137
13	Single-Sign-On-Systeme	139
14	Die Technik hinter Federation	143
14.1	SAML	144
14.1.1	Profile	146
14.1.2	SAML Assertions and Protocols	150
14.1.3	Bindings	153
15	Der Weg zur weltweiten digitalen Identität	157
15.1	i-Names	157
15.2	XRI	158
15.3	Passel	159
16	Maßgebliche Organisationen für IdM-Standards	161
16.1	Liberty Alliance	161
16.2	WS-I	163
16.3	OASIS	164
16.4	Wer steht hinter den Standardisierungsgremien?	164
16.5	SHIBBOLETH	165
Teil 3	Wirtschaftlicher Nutzen	167
17	Sicherheit gewährleisten	169
17.1	Sicherheit der Kunden	170
17.2	Bewertung der Sicherheit: OSSTMM	172
17.2.1	Berechnen der Risk Assessment Values (RAVs)	174
17.3	Wie viel ist ein geringeres Risiko Wert?	177

18	Neue Möglichkeiten schaffen	181
18.1	The Adaptive Enterprise	181
18.2	Kundenzufriedenheit	182
18.3	Neue Geschäftsmodelle	183
18.4	Collaboration	183
18.5	Serviceorientierte Architektur (SOA)	185
19	Compliance	189
19.1	Sarbanes-Oxley Act (SOX)	190
19.2	8. EU-Richtlinie (EuroSOX)	194
19.3	European Data Protection Directive	195
19.4	Basel II	196
19.5	Solvency II	199
19.6	KonTraG	200
19.7	Health Information Portability and Accountability Act (HIPAA)	200
19.8	FISMA	201
19.9	Customer Identification Program (U.S. Patriot Act)	201
19.10	Gramm-Leach Blily Act (GLBA)	201
19.11	Food and Drug Administration Rule 21 CFR11 (FDA)	202
19.12	Was haben alle gemeinsam?	202
20	Werkzeuge zur Umsetzung der Compliance	205
20.1	COSO	205
	20.1.1 Kontrolltätigkeit	206
	20.1.2 Information und Kommunikation	211
20.2	COBIT	211
	20.2.1 Acquire and implement	215
	20.2.2 Deliver and support	216
	20.2.3 Monitor and evaluate	219
	20.2.4 Aufbau der Prozesse	220
20.3	ISO 17799, 27001 und 27002	221
20.4	ISO 20000	232
20.5	IT-Grundschutz-Kataloge des BSI	233
	20.5.1 Bausteinkataloge	234
	20.5.2 Gefährdungskataloge	236
	20.5.3 Maßnahmenkataloge	237

21	Kosten reduzieren	243
21.1	Betriebskosten	244
21.2	Investitionskosten	247
21.3	Prozesskosten	249
22	Business-Case-Berechnung	255
22.1	Methoden zur Business-Case-Berechnung	255
	22.1.1 Payback Period	255
	22.1.2 Return On Investment (ROI)	256
22.2	Aufbau eines Business Case	256
 Anhang		
A	Relevante Dokumente aus den BSI-Grundschutz-Katalogen	263
A.1	Bausteine	263
A.2	Gefährdungskataloge	263
A.3	Maßnahmenkataloge	265
	Dank geht an ...	267
	Quellenverzeichnis	269
	Stichwortverzeichnis	271