



Sebastian Rieger (Autor)

Einheitliche Authentifizierung in heterogenen IT-Strukturen für ein sicheres e-Science Umfeld



Sebastian Rieger

Einheitliche Authentifizierung in heterogenen
IT-Strukturen für ein sicheres e-Science-Umfeld

Band 59



<https://cuvillier.de/de/shop/publications/1736>

Copyright:

Cuvillier Verlag, Inhaberin Annette Jentsch-Cuvillier, Nonnenstieg 8, 37075 Göttingen,
Germany

Telefon: +49 (0)551 54724-0, E-Mail: info@cuvillier.de, Website: <https://cuvillier.de>

Inhaltsverzeichnis

1	Einleitung.....	1
1.1	Problemstellung und Motivation	2
1.2	Zielsetzung	4
1.3	Methodik und Aufbau der Arbeit	4
2	Grundlagen der Authentifizierung in IT-Strukturen.....	6
2.1	Begriffsdefinitionen.....	6
2.1.1	Benutzer.....	6
2.1.2	Betreiber	7
2.1.3	Ressource.....	7
2.1.4	Authentifizierung.....	8
2.1.5	Authentifizierungsmerkmal	8
2.1.6	Authentifizierungsfaktor.....	9
2.1.7	Authentifizierungskonto	9
2.1.8	Authentifizierungsverfahren und -sitzung	10
2.1.9	Authentifizierungssystem	10
2.1.10	Heterogene IT-Strukturen.....	11
2.1.11	Einheitliche Authentifizierung	11
2.1.12	Reduced- und Single Sign-On	12
2.1.13	e-Science.....	13
2.2	Grundwerte für IT-Sicherheit.....	14
2.2.1	Vertraulichkeit.....	14
2.2.2	Integrität	15
2.2.3	Verfügbarkeit.....	15
2.2.4	Verbindlichkeit.....	16
2.2.5	Authentizität	16
2.3	Richtlinien für die Authentifizierung im Rahmen der IT-Sicherheit	17
2.3.1	Internationale Richtlinien für IT-Sicherheit und Authentifizierung.....	17
2.3.2	Rechtliche Grundlagen der IT-Sicherheit und Authentifizierung.....	19
2.4	Authentifizierungsmodelle	20
2.4.1	Authentifizierung in homogenen IT-Strukturen	21
2.4.2	Authentifizierung in heterogenen IT-Strukturen	23
2.5	Authentifizierungsmerkmale und -faktoren	25
2.5.1	Kenntnis einer Information.....	25
2.5.2	Besitz eines Tokens	27
2.5.3	Biometrische Eigenschaft.....	29

2.5.4	Lokation, Zeit	30
2.6	Kryptographie als Basis für Authentifizierungsverfahren.....	31
2.6.1	Symmetrische und asymmetrische Verschlüsselung	31
2.6.2	Digitale Signaturen und Hash-Verfahren	34
2.6.3	Challenge-Response Verfahren	36
2.7	Authentifizierungsverfahren und -systeme	37
2.7.1	Lokale Authentifizierung	37
2.7.2	Direkte Authentifizierung.....	38
2.7.3	Indirekte Authentifizierung	39
2.7.4	Off-line-Authentifizierung	41
2.8	Risiken der Authentifizierung	43
2.8.1	Sicherheit von Authentifizierungsmerkmalen	43
2.8.2	Angriffe auf Authentifizierungsverfahren	47
2.8.3	Angriffe auf Authentifizierungssysteme	50
2.8.4	Social Engineering und Phishing.....	52
3	Authentifizierung in heterogenen IT-Strukturen.....	54
3.1	Diversität der Authentifizierung als Grund für deren Vereinheitlichung.....	54
3.2	Bestehende Lösungen für einheitliche Authentifizierung	56
3.2.1	Verwendung eines einzigen Authentifizierungsverfahrens und -systems	56
3.2.2	Verzeichnisdienste, Meta-Directory und Virtual Directory	58
3.2.3	Kerberos	63
3.2.4	Public-Key-Infrastrukturen	65
3.2.5	Netzwerk-Authentifizierungsprotokolle.....	70
3.2.6	Web-basierte Authentifizierung	73
3.2.7	Federation-basierte Authentifizierung.....	76
3.2.8	Modulare Authentifizierungs-Clients und Proxies	81
3.2.9	Passwort-Speicher und Authentifizierungsautomatismen	84
3.3	Probleme bestehender Lösungen für eine einheitliche Authentifizierung.....	87
3.3.1	Interoperabilität, Flexibilität und Skalierbarkeit	87
3.3.2	Verwaltungsaufwand.....	88
3.3.3	Sicherheit und Benutzbarkeit	89
3.3.4	Fehlende Benutzer-Zentrierung und Datenschutz	90
3.4	Stand der Forschung zu einheitlichen Authentifizierungsverfahren	91
4	Anforderungen an eine einheitliche Authentifizierung in heterogenen IT-Strukturen.....	96
4.1	Ziele einer einheitlichen Authentifizierung.....	96

4.1.1	Vereinheitlichung der Authentifizierungselemente	96
4.1.2	Steigerung von Benutzbarkeit und IT-Sicherheit	97
4.1.3	Einheitliches Identity Management	97
4.2	Betrachtete Zielgruppen	98
4.2.1	Wissenschaftliche IT-Strukturen	99
4.2.2	Betriebliche IT-Strukturen.....	100
4.3	Schnittstellen zu nachgelagerten Verfahren	101
4.3.1	Autorisierung.....	102
4.3.2	Sitzungsverwaltung und Accounting.....	103
4.3.3	Auditing.....	103
4.4	Begrenzende Faktoren.....	104
4.4.1	Homogenität von Authentifizierungsmerkmalen	104
4.4.2	Kompatibilität der angebundenen Ressourcen	105
4.4.3	Portabilität von Authentifizierungsverfahren und -merkmalen	106
4.4.4	Rechtliche Aspekte	107
5	Modellierung und Klassifizierung der Faktoren für eine einheitliche Authentifizierung	108
5.1	Formales Modell für die Authentifizierung in heterogenen IT-Strukturen	109
5.2	Integrationsformen der im Modell ermittelten Faktoren	114
5.3	Sichtweisen auf das Authentifizierungsmodell	116
5.3.1	Sicht der Benutzer	117
5.3.2	Sicht der Organisationen (Betreiber).....	119
5.4	Quantifizierung des Aufwands und der erzielten Sicherheit.....	122
5.4.1	Bestehende Bewertungsmodelle.....	122
5.4.1.1	Aufwand der Authentifizierung als Defizit.....	124
5.4.1.2	Sicherheit der Authentifizierung als Defizit.....	125
5.4.1.3	Berechnung des Gesamtdefizits	126
5.4.2	Erweiterte Bewertung des Aufwands in heterogenen IT-Strukturen.....	128
5.4.2.1	Aufwand für die Verwendung seitens der Benutzer	130
5.4.2.2	Aufwand für die Verwendung seitens der Organisationen	132
5.4.2.3	Aufwand für die Verwaltung seitens der Benutzer	134
5.4.2.4	Aufwand für die Verwaltung seitens der Organisationen	136
5.4.2.5	Berechnung des insgesamt erforderlichen Aufwands	138
5.4.3	Erweiterte Bewertung der Sicherheit in heterogenen IT-Strukturen	141
5.4.3.1	Sicherheit der Authentifizierung in heterogenen IT-Strukturen.....	142
5.4.3.2	Berechnung der insgesamt erzielten Sicherheit	146
5.5	Vereinheitlichung von Authentifizierungsmerkmalen	148
5.5.1	Diversität von Authentifizierungsmerkmalen.....	149

5.5.2	Bewertung des Vereinheitlichungspotentials	152
5.5.3	Ermittlung geeigneter Integrationsformen	159
5.5.3.1	Reduktion der Authentifizierungsmerkmale (Int _a).....	162
5.5.3.2	Integration der Authentifizierungsmerkmale (Int _b).....	163
5.5.3.3	Integration und Reduktion der Relationen (Int _c , Int _d)	164
5.5.4	Grenzen der Vereinheitlichung	165
5.5.5	Resultierende Hypothesen.....	166
5.6	Vereinheitlichung von Authentifizierungsverfahren.....	167
5.6.1	Diversität von Authentifizierungsverfahren	167
5.6.2	Bewertung des Vereinheitlichungspotentials	168
5.6.3	Ermittlung geeigneter Integrationsformen	171
5.6.3.1	Reduktion von Authentifizierungsverfahren (Int _a).....	173
5.6.3.2	Integration von Authentifizierungsverfahren (Int _b)	174
5.6.3.3	Integration und Reduktion der Relationen (Int _c , Int _d)	176
5.6.4	Grenzen der Vereinheitlichung	177
5.6.5	Resultierende Hypothesen.....	177
5.7	Vereinheitlichung von Authentifizierungssystemen	178
5.7.1	Diversität von Authentifizierungssystemen	178
5.7.2	Bewertung des Vereinheitlichungspotentials	179
5.7.3	Ermittlung geeigneter Integrationsformen	181
5.7.3.1	Reduktion von Authentifizierungssystemen (Int _a).....	183
5.7.3.2	Integration von Authentifizierungssystemen (Int _b).....	183
5.7.3.3	Integration und Reduktion der Relationen (Int _c , Int _d)	185
5.7.4	Grenzen der Vereinheitlichung	185
5.7.5	Resultierende Hypothesen.....	186
6	Realisierung einer einheitlichen Authentifizierung für sichere e-Science- Umgebungen	187
6.1	Kriterien für die Optimierung einheitlicher Authentifizierung	188
6.1.1	Minimierung des Aufwands für die Betreiber.....	188
6.1.2	Minimierung des Aufwands für die Benutzer	189
6.1.3	Gewährleistung der IT-Sicherheit	191
6.2	Gestaltung des Authentifizierungsmodells für heterogene IT-Strukturen.....	192
6.2.1	Gestaltung des Verhältnisses zwischen Aufwand und Sicherheit	192
6.2.2	Unschärfe von Aufwand und Sicherheit im Authentifizierungsmodell für heterogene IT-Strukturen	197
6.2.3	Zielfunktion für die Vereinheitlichung des Authentifizierungsmodells.....	204
6.3	Implementierung eines Referenzmodells	207
6.3.1	Kombination bestehender Verfahren für eine einheitliche Authentifizierung	207

6.3.2	Erweiterung bestehender Lösungen.....	212
6.3.2.1	Skalierbares Identity Management.....	212
6.3.2.2	Web-basierte „Identity Management“-Portale.....	213
6.3.2.3	Self-Service PKI-Lösungen für e-Science.....	215
6.3.2.4	Integration Federation-basierter Authentifizierung in Desktop-Anwendungen.....	217
6.3.2.5	Flexible Trust-Modelle.....	220
6.3.3	Ebenenmodell für einheitliche Authentifizierung.....	221
6.3.4	Integrationsstrategie für einheitliche Authentifizierung.....	224
6.4	Fallstudien im Kooperationsprojekt GÖ*.....	228
6.4.1	Identity Management am Wissenschaftsstandort Göttingen.....	230
6.4.2	PKI für die Max-Planck-Gesellschaft und Universität Göttingen.....	232
6.4.3	Zusammenfassung der Ergebnisse der Fallstudien.....	235
6.5	Bewertung des Realisierungsansatzes.....	238
6.5.1	Quantifizierung der erzielten Vereinheitlichung.....	239
6.5.1.1	Bewertung der Ausgangssituation.....	239
6.5.1.2	Bewertung nach der Realisierung eines Identity Managements.....	241
6.5.1.3	Bewertung nach der Realisierung exemplarischer „Single Sign-On“-Lösungen.....	243
6.5.1.4	Bewertung nach der Realisierung einer Public-Key-Infrastruktur... ..	243
6.5.1.5	Bewertung nach der exemplarischen Verwendung von Tokens.....	245
6.5.2	Abgrenzung zu homogenen IT-Strukturen.....	247
7	Fazit und Ausblick.....	249
7.1	Zusammenfassung der Ergebnisse.....	249
7.2	Zukünftige Arbeiten.....	251
	Abbildungsverzeichnis.....	253
	Tabellenverzeichnis.....	256
	Literaturverzeichnis.....	258