

# Inhaltsverzeichnis

<b>I Kerberos</b>	<b>1</b>
<b>1 Kerberos im Überblick .....</b>	<b>3</b>
1.1 Ursprung am MIT: Das Athena-Projekt .....	3
1.2 Versionen des Kerberos-Protokolls .....	5
1.3 Standardisierung.....	5
1.4 Implementierungen.....	6
1.4.1 Kerberos v4 .....	6
1.4.2 Kerberos v5 .....	7
1.4.3 Interoperabilität .....	8
<b>2 Grundlagen der Netzwerkauthentisierung mit Kerberos</b>	<b>9</b>
2.1 Authentisierung .....	9
2.1.1 Authentisierungsmerkmale .....	10
2.1.2 Problematik der Passwörter .....	12
2.1.3 Lokale Anmeldung vs. Netzwerkauthentisierung ....	13
2.2 Authentisierung mit Kerberos .....	15
2.2.1 KDC.....	15
2.2.2 Realm .....	16
2.2.3 Principals.....	16
2.2.4 Tickets .....	17
2.2.5 Gegenseitige Authentisierung.....	18
2.2.6 Lokale Anmeldung und Kerberos.....	18
2.3 Delegation .....	19
2.4 Autorisierung, Zugriffskontrolle und Namensdienste .....	20
2.4.1 Authentisierung ist Voraussetzung .....	21
2.4.2 Dienste und Identitäten.....	21
2.4.3 Autorisierung und Kerberos .....	22
2.5 Single Sign-on (SSO) .....	23
2.6 Zusammenfassung .....	25

<b>3</b>	<b>Kerberos aus Anwendersicht .....</b>	<b>27</b>
3.1	Die Beispielumgebung .....	27
3.2	Lokale Anmeldung .....	28
3.3	Der Credential Cache .....	29
3.4	Anmeldung an Netzwerkdiensten .....	30
3.5	Delegation .....	32
3.6	Eine Demo-Webseite .....	34
3.7	Umgang mit dem Credential Cache .....	40
3.8	Zusammenfassung .....	41
<b>4</b>	<b>Sicherheit und Kryptografie .....</b>	<b>43</b>
4.1	Sicherheitsüberlegungen .....	43
4.1.1	Allgemeine Sicherheitsanforderungen .....	43
4.1.2	Die beteiligten Systemkomponenten .....	44
4.1.3	Anforderungen an Kerberos .....	47
4.2	Kryptografie in der Netzwerksicherheit .....	50
4.2.1	Vertraulichkeit .....	50
4.2.2	Integrität .....	53
4.2.3	Authentisierung .....	54
4.2.4	Passwörter, Schlüssel und Schlüsselaustausch .....	59
4.2.5	Zusammenfassung .....	63
<b>5</b>	<b>Wie funktioniert Kerberos v5? .....</b>	<b>65</b>
5.1	Das Funktionsprinzip im Überblick .....	65
5.1.1	Voraussetzungen .....	65
5.1.2	Das einstufige Kerberos-Verfahren .....	67
5.1.3	Diskussion .....	70
5.1.4	Das zweistufige Kerberos-Verfahren .....	71
5.1.5	Zusammenfassung .....	74
5.2	Das Funktionsprinzip im Detail .....	75
5.2.1	Die KDC-Datenbank .....	76
5.2.2	Der Authentication Service (AS) .....	76
5.2.3	Zugriff auf kerberisierte Dienste .....	81
5.2.4	Der Ticket-Granting Service (TGS) .....	85
5.3	Zusammenfassung .....	88
<b>6</b>	<b>Kerberos für Fortgeschrittene .....</b>	<b>91</b>
6.1	KDC-Optionen .....	91
6.1.1	Optionen für Ticket Renewing .....	92
6.1.2	Optionen für Ticket Postdating .....	92
6.1.3	Optionen für die Kerberos-Delegation .....	93
6.1.4	Sonstige Optionen .....	93

6.2	Ticket Flags .....	94
6.2.1	Flags für Ticket Renewing .....	94
6.2.2	Flags für Ticket Postdating .....	94
6.2.3	Flags für die Kerberos-Delegation .....	95
6.2.4	Sonstige Flags .....	95
6.3	AP-Optionen.....	96
6.4	Tickets automatisiert erneuern .....	96
6.5	Tickets für die Zukunft .....	99
6.6	Delegation zum Ersten .....	101
6.6.1	Ticket Forwarding .....	101
6.6.2	Ticket Proxying .....	103
6.7	Authentisierung zwischen Realms .....	105
6.7.1	Grundsätzliches zu Vertrauensstellung.....	105
6.7.2	Zwei Realms .....	107
6.7.3	Mehr als zwei Realms .....	109
6.8	Namenskanonisierung und Referrals .....	112
6.8.1	Kanonisierung der Client-Principal-Namen .....	113
6.8.2	Kanonisierung der Dienste-Principal-Namen .....	114
6.8.3	Verweise an entfernte Realms .....	115
6.9	Kerberos und Autorisierungsdaten.....	115
6.10	User-to-User-Authentisierung .....	116
6.11	Delegation zum Zweiten .....	117
6.11.1	Constrained Delegation .....	118
6.11.2	Protocol Transition.....	119
6.11.3	Diskussion.....	120
6.12	Initiale Authentisierung mit Zertifikaten .....	121
6.12.1	Eine Lösung für die Passwort-Problematik .....	121
6.12.2	Das Funktionsprinzip von PKINIT .....	122
6.12.3	Fazit .....	123

## II Zentrale Infrastrukturen 125

7	<b>Grundlegende Infrastruktur .....</b>	<b>129</b>
7.1	Überblick .....	129
7.2	DNS-Namensaüflösung mit BIND .....	130
7.2.1	BIND installieren .....	131
7.2.2	Zonen einrichten .....	131
7.2.3	Starten und Testen .....	133
7.3	Zeitsynchronisation mit NTP.....	133

7.4	Certificate Authority (CA) mit OpenSSL .....	134
7.4.1	Einrichtung der CA .....	134
7.4.2	Einen Zertifikats-Request erzeugen .....	136
7.4.3	Das Zertifikat unterschreiben .....	137
7.5	Verzeichnisdienst mit OpenLDAP .....	139
7.5.1	Installation und Konfiguration.....	139
7.5.2	LDAP-Datenbank für dc=example,dc=com .....	142
7.5.3	Ein erster Test .....	144
7.5.4	Sicherheit .....	145
<b>8</b>	<b>Das Key Distribution Center von MIT Kerberos .....</b>	<b>149</b>
8.1	Übersicht .....	149
8.2	Softwareinstallation .....	149
8.3	Konfiguration .....	150
8.3.1	Der Master Key der KDC-Datenbank .....	150
8.3.2	Zeitangaben bei MIT Kerberos .....	151
8.3.3	Verschlüsselungstypen.....	152
8.3.4	Die Datei kdc.conf .....	152
8.4	Initialisierung der KDC-Datenbank .....	157
8.4.1	Die Datenbank mit kdb5_util initialisieren .....	157
8.4.2	Die initiale Datenbank .....	159
8.4.3	Mit kadmin.local weitere Principals anlegen .....	160
8.4.4	Master Key in Stash-Datei ablegen .....	161
8.5	Starten des KDC .....	163
8.6	Ein erster Test.....	163
<b>9</b>	<b>Die Administration von MIT Kerberos .....</b>	<b>165</b>
9.1	Der Kadmin-Dienst.....	165
9.2	Administrative Zugriffe kontrollieren.....	167
9.3	Der Kpasswd-Dienst.....	169
9.4	Starten der administrativen Dienste .....	169
9.5	Principals verwalten.....	171
9.5.1	Passwortrichtlinien .....	171
9.5.2	Principal-Eigenschaften .....	174
9.5.3	Anwender-Principals anlegen .....	179
9.5.4	Dienste-Principals anlegen .....	181
9.5.5	Verschlüsselungstypen der Principals verwalten ....	182
9.6	Keytabs verwalten .....	183
9.7	Service Keys ändern .....	184

<b>10</b>	<b>Die Clientkommandos von MIT Kerberos .....</b>	<b>187</b>
10.1	Installation und Konfiguration .....	187
10.2	Die Kommandos kinit und klist .....	187
10.2.1	Tickets holen .....	187
10.2.2	Ticket-Eigenschaften anzeigen und beeinflussen....	189
10.2.3	Protokoll-Requests beeinflussen .....	191
10.2.4	Sonstige Kommandozeilenoptionen .....	191
10.2.5	Service Tickets holen .....	192
10.2.6	Mit Keytabs arbeiten .....	192
10.3	Das Kommando kvno .....	194
10.4	Das Kommando kpasswd .....	195
10.5	Das Kommando kdestroy.....	196
10.6	Die Kommandos k5start und krenew .....	196
10.6.1	krenew .....	196
10.6.2	k5start .....	197
<b>11</b>	<b>Die Konfiguration der MIT Libraries .....</b>	<b>199</b>
11.1	Die Datei krb5.conf .....	199
11.1.1	Die Struktur der krb5.conf .....	200
11.1.2	Konfigurationsabschnitte .....	201
11.1.3	Parameter im Abschnitt [libdefaults] .....	202
11.1.4	Parameter im Abschnitt [realms] .....	206
11.1.5	Parameter im Abschnitt [domain_realm] .....	208
11.1.6	Parameter im Abschnitt [appdefaults] .....	209
11.1.7	Parameter im Abschnitt [logging] .....	211
11.1.8	Die krb5.conf für den Realm EXAMPLE.COM.....	211
11.2	Konfiguration über DNS .....	212
11.2.1	SRV Records .....	212
11.2.2	TXT Records .....	215
11.3	Konfiguration mit Umgebungsvariablen .....	215
<b>12</b>	<b>Ausfallsicherheit für MIT Kerberos .....</b>	<b>217</b>
12.1	Backup der KDC-Datenbank .....	217
12.2	Wiederherstellung der KDC-Datenbank .....	218
12.3	Replikation der KDC-Datenbank .....	219
12.3.1	Möglichkeiten der Kerberos-Replikation .....	219
12.3.2	Sicherheit der Replikation.....	220
12.4	Replikation bei MIT Kerberos .....	220
12.4.1	Ein Slave KDC einrichten .....	221
12.4.2	Schritte auf dem Master KDC.....	223
12.4.3	Das Slave KDC starten .....	224
12.4.4	Das Slave KDC bekannt machen.....	224
12.4.5	Regelmäßig replizieren .....	224

<b>13</b>	<b>Ein LDAP-Backend für die MIT-Datenbank .....</b>	<b>227</b>
13.1	Überblick .....	227
	13.1.1 Erweiterte Funktionalitäten .....	227
	13.1.2 Vorgehensweise .....	228
	13.1.3 Sicherheit .....	228
13.2	Software, Schema und Objekte .....	230
	13.2.1 Software installieren .....	230
	13.2.2 Das Schema erweitern .....	230
	13.2.3 Konvention .....	233
	13.2.4 Objekte anlegen .....	234
	13.2.5 Limits für LDAP-Suchvorgänge .....	235
	13.2.6 LDAP-Berechtigungen .....	236
13.3	Das KDC auf LDAP umstellen .....	236
	13.3.1 Vorbereitungen .....	236
	13.3.2 Konfiguration .....	237
	13.3.3 Die KDC-Datenbank im LDAP initialisieren .....	239
	13.3.4 Den Realm einrichten .....	241
13.4	Existierende Nutzerobjekte .....	242
13.5	Principal-Aliase .....	245
	13.5.1 Client-Aliase .....	246
	13.5.2 Dienste-Aliase .....	247
13.6	Ausfallsicherheit mit LDAP .....	247
	13.6.1 OpenLDAP auf kdc01 vorbereiten .....	248
	13.6.2 LDAP-Server auf kdc02 einrichten .....	253
	13.6.3 Ausfallsicherheit für das KDC .....	255
	13.6.4 Die Clientkonfiguration anpassen .....	256
13.7	Lockout Policies .....	257
<b>14</b>	<b>Einen Heimdal Realm einrichten .....</b>	<b>261</b>
14.1	Überblick .....	261
14.2	Vorbereitung .....	262
14.3	Das Key Distribution Center von Heimdal .....	263
	14.3.1 Die Datei kdc.conf .....	264
	14.3.2 Master Key .....	266
	14.3.3 Die KDC-Datenbank initialisieren .....	267
	14.3.4 Das KDC starten .....	269
14.4	Die Administration von Heimdal .....	269
	14.4.1 Administrative Zugriffe kontrollieren .....	269
	14.4.2 Principals verwalten .....	270
	14.4.3 Weitere administrative Tätigkeiten .....	273
	14.4.4 Passwörter verwalten .....	273
14.5	Die Heimdal-Werkzeuge .....	275

14.6	Ausfallsicherheit für Heimdal .....	276
14.6.1	Ein Slave KDC einrichten .....	277
14.6.2	Starten des hpropd auf dem Slave KDC .....	278
14.6.3	Die Replikation mit Hprop starten .....	278
14.6.4	Regelmäßig replizieren .....	278
14.7	Ein LDAP-Backend für Heimdal .....	279
14.7.1	LDAP vorbereiten .....	279
14.7.2	Das KDC auf LDAP umstellen .....	281
14.7.3	Ausfallsicherheit mit LDAP .....	282
<b>15</b>	<b>Kerberos bei Microsoft Active Directory .....</b>	<b>285</b>
15.1	Active Directory im Überblick .....	285
15.1.1	Kerberos in Active Directory .....	286
15.1.2	AD-Version und Functional Level .....	287
15.2	Testlabor .....	288
15.3	Das Key Distribution Center von Active Directory .....	289
15.3.1	Die Domäne einrichten .....	289
15.3.2	Grundlegende Dienste .....	295
15.3.3	Ein erster Test .....	296
15.3.4	Ausfallsicherheit .....	297
15.4	Kerberos-Administration .....	297
15.4.1	Administrationswerkzeuge .....	298
15.4.2	Überblick über den neuen Realm .....	298
15.4.3	Principals verwalten .....	300
15.4.4	Verschlüsselungstypen .....	306
15.4.5	Keytabs erzeugen .....	307
15.4.6	Kerberos Policies .....	309
15.5	Kerberos-Administration mit LDAP .....	311
15.5.1	LDAP-Suchen im AD .....	312
15.5.2	Ein Benutzerobjekt anlegen .....	313
15.5.3	Diensteobjekte anlegen .....	315
15.5.4	Maschinenobjekte anlegen .....	315
15.6	Weitere Werkzeuge .....	318
<b>16</b>	<b>Kerberos für Fortgeschrittene .....</b>	<b>319</b>
16.1	Verteilte Kerberos-Umgebungen .....	319
16.1.1	Cross-Realm bei MIT Kerberos .....	320
16.1.2	Cross-Realm bei Heimdal .....	325
16.1.3	Cross-Realm bei Active Directory .....	329
16.1.4	Aufbau der Gesamtstruktur .....	331

16.2	Delegation für Fortgeschrittene .....	336
16.2.1	Vorbereitungen.....	336
16.2.2	Das Ok-As-Delegate Flag .....	337
16.2.3	kimpersonate.....	339
16.2.4	Constrained Delegation und Protocol Transition .....	341
16.3	PKINIT .....	344
16.3.1	Initiale Authentisierung mit Zertifikaten .....	344
16.3.2	PKINIT im Testnetz.....	345
16.3.3	Kerberos, PKINIT und Smartcards .....	350
<b>III</b>	<b>Integrierte Umgebungen</b>	<b>355</b>
<b>17</b>	<b>Grundlagen .....</b>	<b>359</b>
17.1	Principals und Keytabs verwalten.....	359
17.1.1	Client Principals anlegen .....	359
17.1.2	Funktionalität von Client Principals prüfen .....	360
17.1.3	Dienste-Principals anlegen .....	361
17.1.4	Funktionalität von Dienste-Principals prüfen .....	362
17.1.5	Keytab-Dateien anlegen .....	362
17.1.6	Funktionalität von Keytab-Dateien prüfen .....	363
17.2	Zwischenstand.....	363
17.3	Die nativen Kerberos-Bibliotheken.....	364
17.4	GSS-API .....	364
17.5	SPNEGO .....	366
17.6	SSPI .....	366
17.7	SASL .....	367
17.7.1	Protokolle .....	367
17.7.2	Mechanismen .....	367
17.7.3	Konzepte .....	368
17.7.4	Cyrus SASL .....	369
17.8	Zusammenfassung .....	370
<b>18</b>	<b>LDAP-Infrastruktur .....</b>	<b>371</b>
18.1	LDAP im Überblick .....	371
18.1.1	Begriffe und Standards .....	371
18.1.2	Serverimplementierungen .....	373
18.1.3	Daten Im LDAP .....	373
18.1.4	Verzeichnisoperationen .....	375
18.2	LDAP-Sicherheit .....	376
18.3	Kerberisierung bei Active Directory .....	377

18.4	Kerberisierung bei OpenLDAP .....	379
18.4.1	SASL-Konfiguration .....	379
18.4.2	Principal und Keytab.....	380
18.4.3	Identitäts-Mapping .....	381
18.5	Zusammenfassung .....	384
<b>19</b>	<b>Client-Anbindung .....</b>	<b>387</b>
19.1	Windows-Clients in Active Directory .....	387
19.2	Ausbau der Gesamtstruktur .....	390
19.2.1	LDAP-Referrals einrichten .....	391
19.2.2	Identitäts- und Autorisierungsdaten für Linux.....	392
19.3	Linux-Clients in der Infrastruktur mit Kerberos und OpenLDAP	397
19.3.1	Name Service Switch (NSS).....	398
19.3.2	NSS-Module für LDAP.....	399
19.3.3	Pluggable Authentication Modules (PAM).....	406
19.3.4	pam-krb5 .....	409
19.4	Linux-Clients in Active Directory .....	412
19.5	Linux-Clients in der Gesamtinfrastruktur .....	413
19.5.1	Problemstellung .....	413
19.5.2	slapd als lokaler LDAP-Proxy .....	414
19.5.3	slapd-Konfiguration.....	415
19.5.4	Test der NSS-Anbindung .....	418
19.5.5	PAM-Kerberos-Konfiguration .....	419
19.5.6	Ausblick .....	421
19.6	Zusammenfassung .....	421
<b>20</b>	<b>Elementare Netzwerkdienste unter Unix und Linux ....</b>	<b>423</b>
20.1	Traditionelle Remote-Dienste .....	423
20.1.1	Telnet .....	423
20.1.2	Kerberisierte Remote Shell: krb5-rsh.....	430
20.1.3	Kerberisierter File Transfer: krb5-ftp .....	431
20.2	Moderne Remote-Dienste mit OpenSSH .....	432
20.2.1	Vorbereitungen.....	433
20.2.2	Kerberisierte Secure-Shell-Sitzung .....	434
20.2.3	Tickets weiterleiten .....	435
20.2.4	Secure-Shell-Client unter Windows .....	436
20.2.5	OpenSSH ohne Kerberos Tickets .....	440
20.3	Remote-Dienste in verteilter Umgebung .....	441
20.3.1	Cross-Realm-Problematik .....	441
20.3.2	auth_to_local-Mappings .....	442
20.3.3	Heimdal .....	444
20.3.4	Cross-Realm-Anmeldung ohne Kerberos Tickets .....	444

<b>21</b>	<b>Kerberisierte Dateisysteme .....</b>	<b>445</b>
21.1	CIFS .....	445
21.1.1	CIFS-Service unter Windows einrichten .....	445
21.1.2	Authentisierung bei CIFS.....	448
21.1.3	CIFS-Client unter Linux.....	448
21.1.4	CIFS-Service unter Linux: Samba .....	450
21.1.5	ID Mapping .....	453
21.1.6	Heimatverzeichnisse für alle Windows-Nutzer.....	458
21.2	NFS .....	459
21.2.1	Überblick.....	459
21.2.2	NFSv3 ohne Kerberos .....	460
21.2.3	NFSv3 und Sicherheit .....	462
21.2.4	NFSv4 .....	463
21.2.5	Kerberisierter NFSv4-Service unter Linux .....	464
21.2.6	Den Server einrichten.....	469
21.2.7	Kerberisierter NFSv4-Client unter Linux .....	470
21.2.8	Den Client einrichten .....	471
21.2.9	NFSv4 und Sicherheit .....	473
21.2.10	NFSv4 in Cross-Realm-Umgebung .....	474
21.2.11	Abschlussarbeiten .....	474
<b>22</b>	<b>Single Sign-on für den Apache-Webserver .....</b>	<b>477</b>
22.1	Kerberos und das HTTP-Protokoll .....	477
22.1.1	Das World Wide Web .....	477
22.1.2	Authentisierung im HTTP-Protokoll.....	478
22.1.3	Negotiate (SPNEGO) .....	479
22.2	Den Apache-Server konfigurieren .....	479
22.2.1	Voraussetzungen .....	479
22.2.2	Principals und Keytab-Einträge .....	481
22.2.3	mod_auth_kerb konfigurieren .....	484
22.3	Browserkonfiguration .....	485
22.3.1	Vertrauenswürdige Seiten konfigurieren .....	485
22.3.2	Zugriff testen.....	486
22.3.3	Delegation konfigurieren .....	488
22.3.4	Delegation testen .....	489
22.4	Autorisierungsdaten und Ticket-Größe.....	491
22.5	Autorisierung über LDAP.....	492
22.6	Beispiel MediaWiki .....	495
22.6.1	Die Anwendung einrichten .....	495
22.6.2	Kerberisierung .....	496
22.7	Zusammenfassung .....	498

<b>IV Anhang</b>	<b>499</b>
<b>A Schnelleinstieg in LDAP .....</b>	<b>501</b>
A.1 LDIF .....	501
A.1.1 Das LDAP-Datenmodell .....	501
A.1.2 LDIF-Repräsentation von LDAP-Daten .....	502
A.1.3 Änderungen mit LDIF .....	503
A.2 OpenLDAP-Tools .....	505
A.2.1 Suchen mit ldapsearch .....	505
A.2.2 Authentisierung .....	506
A.2.3 Weitere OpenLDAP-Kommandos .....	508
A.3 Grafische LDAP-Werkzeuge .....	508
<b>B Konfiguration der Betriebssysteme.....</b>	<b>511</b>
B.1 Netzwerkparameter .....	511
B.2 Ubuntu 10.04 .....	511
B.3 Windows Server 2008 R2 .....	514
B.4 Windows 7 .....	515
<b>C Softwareinstallationen .....</b>	<b>517</b>
C.1 Vorbemerkungen .....	517
C.2 MIT Kerberos .....	518
C.3 MIT-Kerberos-Applikationen .....	519
C.4 Heimdal .....	519
C.5 k5start.....	520
C.6 msktutil .....	521
C.7 OpenSC .....	521
<b>Literaturverzeichnis .....</b>	<b>523</b>
<b>Index .....</b>	<b>529</b>