

Inhaltsverzeichnis

I	Kerberos	1
1	Kerberos im Überblick	3
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 und Kompatibilität	8
2	Grundlagen der Netzwerkauthentisierung mit Kerberos	11
2.1	Authentisierung	11
2.1.1	Authentisierungsmerkmale	12
2.1.2	Problematik der Passwörter	14
2.1.3	Lokale Anmeldung vs. Netzwerkauthentisierung	15
2.2	Authentisierung mit Kerberos	17
2.2.1	Key Distribution Center	17
2.2.2	Realm	18
2.2.3	Principals	18
2.2.4	Tickets	19
2.2.5	Gegenseitige Authentisierung	20
2.2.6	Lokale Anmeldung und Kerberos	20
2.3	Delegation	20
2.4	Autorisierung und Zugriffskontrolle	22
2.4.1	Authentisierung ist Voraussetzung	23
2.4.2	Identity Mappings	23
2.4.3	Autorisierung und Kerberos	24
2.5	Single Sign-on (SSO)	25
2.6	Zusammenfassung	27

3	Kerberos aus Anwendersicht	29
3.1	Die Beispielumgebung	29
3.2	Lokale Anmeldung	30
3.3	Der Credential Cache	31
3.4	Anmeldung an Netzwerkdiensten	32
3.5	Delegation	34
3.6	Eine Demo-Webseite	36
3.7	Umgang mit dem Credential Cache	41
3.8	Zusammenfassung	42
4	Sicherheit und Kryptografie	45
4.1	Sicherheitsüberlegungen	45
4.1.1	Allgemeine Sicherheitsanforderungen	45
4.1.2	Die beteiligten Systemkomponenten	46
4.1.3	Anforderungen an Kerberos	49
4.2	Kryptografie in der Netzwerksicherheit	52
4.2.1	Vertraulichkeit	52
4.2.2	Integrität	55
4.2.3	Authentisierung	56
4.2.4	Passwörter, Schlüssel und Schlüsselaustausch	61
4.2.5	Zusammenfassung	67
5	Wie funktioniert Kerberos V5?	69
5.1	Das Funktionsprinzip im Überblick	69
5.1.1	Voraussetzungen	69
5.1.2	Das einstufige Kerberos-Verfahren	71
5.1.3	Diskussion	74
5.1.4	Das zweistufige Kerberos-Verfahren	75
5.1.5	Zusammenfassung	78
5.2	Das Funktionsprinzip im Detail	79
5.2.1	Die KDC-Datenbank	80
5.2.2	Der Authentication Service (AS)	80
5.2.3	Zugriff auf kerberisierte Dienste	86
5.2.4	Der Ticket-Granting Service (TGS)	89
5.3	Zusammenfassung	93
6	Kerberos für Fortgeschrittene	95
6.1	KDC-Optionen	96
6.1.1	Optionen für Ticket Renewing	96
6.1.2	Optionen für Ticket Postdating	96
6.1.3	Optionen für die Kerberos-Delegation	97
6.1.4	Sonstige Optionen	97

6.2	Ticket Flags	98
6.2.1	Flags für Ticket Renewing	98
6.2.2	Flags für Ticket Postdating	98
6.2.3	Flags für die Kerberos-Delegation	99
6.2.4	Sonstige Flags	99
6.3	AP-Optionen	100
6.4	Tickets automatisiert erneuern	100
6.5	Tickets für die Zukunft	103
6.6	Delegation zum Ersten	105
6.6.1	Ticket Forwarding	105
6.6.2	Ticket Proxying	107
6.7	Authentisierung zwischen Realms	109
6.7.1	Grundsätzliches zu Vertrauensstellung	109
6.7.2	Zwei Realms	111
6.7.3	Mehr als zwei Realms	112
6.8	Namenskanonisierung und Referrals	116
6.8.1	Kanonisierung der Client-Principal-Namen	117
6.8.2	Kanonisierung der Dienste-Principal-Namen	118
6.8.3	Verweise an entfernte Realms	119
6.9	User-to-User-Authentisierung	119
6.10	Kerberos und Autorisierungsdaten	120
6.11	Die S4U2Self-Erweiterung	121
6.12	Delegation zum Zweiten	122
6.12.1	Constrained Delegation	123
6.12.2	Protocol Transition	124
6.12.3	Diskussion	125
6.13	Initiale Authentisierung mit Zertifikaten	126
6.13.1	Eine Lösung für die Passwort-Problematik	126
6.13.2	Das Funktionsprinzip von PKINIT	127
6.13.3	Anonymes PKINIT	128
6.13.4	PKINIT Freshness Extension	128
6.13.5	Fazit	129
6.14	FAST: zusätzlicher Schutz für KDC-Austausch	129
6.15	Kerberos über HTTPS	130
6.16	Initiale Authentisierung mit zweitem Faktor	131

II Zentrale Infrastrukturen

133

7	Grundlegende Infrastruktur	137
7.1	Überblick	137
7.2	Software, Systemdienste und lokale Firewall	138

7.3	DNS-Namensauflösung mit BIND	139
7.3.1	BIND installieren	140
7.3.2	Zonen einrichten	140
7.3.3	Starten und Testen	143
7.3.4	Subdomänen	144
7.4	Zeitsynchronisation mit NTP	144
7.5	Certificate Authority (CA) mit OpenSSL	145
7.5.1	Einrichtung der CA	145
7.5.2	Einen Zertifikatsrequest erzeugen	146
7.5.3	Das Zertifikat unterschreiben	148
7.6	Verzeichnisdienst mit OpenLDAP	149
7.6.1	Installation und Grundkonfiguration	150
7.6.2	Schemadefinition	152
7.6.3	Datenbank für dc=example,dc=com konfigurieren ..	153
7.6.4	Datenbank für dc=example,dc=com befüllen	154
7.6.5	Ein erster Test	156
7.6.6	Sicherheit	157
8	Das Key Distribution Center von MIT Kerberos	161
8.1	Übersicht	161
8.2	Softwareinstallation	161
8.3	Konfiguration	162
8.3.1	Der Master Key der KDC-Datenbank	162
8.3.2	Zeitangaben bei MIT Kerberos	163
8.3.3	Verschlüsselungstypen	164
8.3.4	Die Datei kdc.conf	164
8.4	Initialisierung der KDC-Datenbank	170
8.4.1	Die Datenbank mit kdb5_util initialisieren	170
8.4.2	Die initiale Datenbank	171
8.4.3	Mit kadmind.local weitere Principals anlegen	173
8.4.4	Master Key in Stash-Datei ablegen	174
8.5	Ein erster Test	176
9	Die Administration von MIT Kerberos	179
9.1	Der Kadmind-Dienst	179
9.2	Administrative Zugriffe kontrollieren	181
9.3	Der Kpasswd-Dienst	183
9.4	Starten der administrativen Dienste	184
9.5	Principals verwalten	185
9.5.1	Passwortrichtlinien	185
9.5.2	Lockout Policies	189
9.5.3	Principal-Eigenschaften	191

9.5.4	Principals für Anwender:innen anlegen	196
9.5.5	Principals für Dienste anlegen	198
9.5.6	Verschlüsselungstypen der Principals verwalten	199
9.6	Keytabs verwalten	200
9.6.1	Keytabs mit kadmin verwalten	200
9.6.2	Keytabs mit ktutil verwalten	201
9.7	Service Keys ändern	204
10	Die Clientkommandos von MIT Kerberos	207
10.1	Installation und Konfiguration	207
10.2	Die Kommandos kinit und klist	207
10.2.1	Tickets holen	207
10.2.2	Den Credential Cache auswählen	209
10.2.3	Ticket-Eigenschaften anzeigen und beeinflussen	211
10.2.4	Protokollrequests beeinflussen	213
10.2.5	Sonstige Kommandozeilenoptionen	214
10.2.6	Service Tickets holen	214
10.2.7	Mit Keytabs arbeiten	215
10.3	Das Kommando kvno	216
10.4	Das Kommando kpasswd	218
10.5	Das Kommando kdestroy	219
10.6	Die Kommandos k5start und krenew	219
10.6.1	krenew	219
10.6.2	k5start	220
11	Die Konfiguration der MIT Libraries	221
11.1	Die Datei krb5.conf	221
11.1.1	Die Struktur der krb5.conf	222
11.1.2	Konfigurationsabschnitte	223
11.1.3	Parameter im Abschnitt [libdefaults]	224
11.1.4	Parameter im Abschnitt [realms]	228
11.1.5	Parameter im Abschnitt [domain_realm]	230
11.1.6	Parameter im Abschnitt [appdefaults]	231
11.1.7	Die krb5.conf für den Realm EXAMPLE.COM	233
11.2	Konfiguration über DNS	234
11.2.1	SRV Records	234
11.2.2	TXT Records	236
11.3	Konfiguration mit Umgebungsvariablen	237
12	Ausfallsicherheit für MIT Kerberos	239
12.1	Backup der KDC-Datenbank	239
12.2	Wiederherstellung der KDC-Datenbank	240

12.3	Replikation der KDC-Datenbank	241
12.3.1	Möglichkeiten der Kerberos-Replikation	241
12.3.2	Sicherheit der Replikation	242
12.4	Replikation bei MIT Kerberos	242
12.4.1	Ein Replica KDC einrichten	243
12.4.2	Schritte auf dem Master KDC	245
12.4.3	Das Replica KDC starten	245
12.4.4	Das Replica KDC bekannt machen	246
12.4.5	Regelmäßig replizieren	246
13	Ein LDAP-Backend für die MIT-Datenbank	249
13.1	Überblick	249
13.1.1	Erweiterte Funktionalitäten	249
13.1.2	Vorgehensweise	250
13.1.3	Sicherheit	250
13.2	Software, Schema und Konfiguration des LDAP-Servers	252
13.2.1	Software installieren	252
13.2.2	Das Schema erweitern	252
13.3	Das KDC auf LDAP umstellen	256
13.3.1	Vorbereitungen	256
13.3.2	Konfiguration	257
13.3.3	Die KDC-Datenbank im LDAP initialisieren	259
13.3.4	Den Realm einrichten	260
13.4	Existierende Nutzerobjekte	261
13.5	Principal-Aliase	264
13.5.1	Client-Aliase	264
13.5.2	Dienste-Aliase	266
13.6	Ausfallsicherheit mit LDAP	267
13.6.1	OpenLDAP auf kdc01 vorbereiten	268
13.6.2	LDAP-Server auf kdc02 einrichten	274
13.6.3	Ausfallsicherheit für das KDC	276
13.6.4	Die Clientkonfiguration anpassen	277
14	Einen Heimdal Realm einrichten	279
14.1	Überblick	279
14.2	Vorbereitung	280
14.3	Das Key Distribution Center von Heimdal	281
14.3.1	Die Datei kdc.conf	282
14.3.2	Master Key	284
14.3.3	Die KDC-Datenbank initialisieren	285
14.3.4	Das KDC starten	287
14.4	Die Administration von Heimdal	287
14.4.1	Administrative Zugriffe kontrollieren	287

14.4.2	Principals verwalten	288
14.4.3	Weitere administrative Tätigkeiten	291
14.4.4	Passwörter verwalten	292
14.5	Die Heimdal-Werkzeuge	293
14.6	Ausfallsicherheit für Heimdal	294
14.6.1	Ein Replica KDC einrichten	295
14.6.2	Starten des hpropd auf dem Replica KDC	296
14.6.3	Die Replikation mit Hprop starten	296
14.6.4	Regelmäßig replizieren	297
14.7	Ein LDAP-Backend für Heimdal	298
14.7.1	LDAP vorbereiten	298
14.7.2	Das KDC auf LDAP umstellen	300
14.7.3	Ausfallsicherheit mit LDAP	301
15	Kerberos bei Microsoft Active Directory	303
15.1	Active Directory im Überblick	304
15.1.1	Kerberos in Active Directory	304
15.1.2	Kerberos-Erweiterungen	305
15.1.3	AD-Version und Functional Level	305
15.2	Testlabor	307
15.3	Das Key Distribution Center von Active Directory	308
15.3.1	Die Domäne einrichten	308
15.3.2	Grundlegende Dienste	313
15.3.3	Ein erster Test	314
15.3.4	Ausfallsicherheit	316
15.4	Kerberos-Administration	317
15.4.1	Administrationswerkzeuge	317
15.4.2	Überblick über den neuen Realm	319
15.4.3	Principals verwalten	320
15.4.4	Verschlüsselungstypen	326
15.4.5	Kerberos Policies	329
15.5	Keytab-Verwaltung in AD-Infrastrukturen	331
15.5.1	Keytabs unter Windows mit ktpass.exe erzeugen	331
15.5.2	Host Keytabs unter Linux mit adcli verwalten	333
15.5.3	Host Keytabs unter Linux mit msktutil verwalten	334
15.5.4	Keytabs für Service Accounts unter Linux mit msktutil verwalten	336
15.6	Kerberos-Administration mit LDAP	337
15.6.1	LDAP-Suchen im AD	338
15.6.2	Ein Benutzerobjekt anlegen	340
15.6.3	Diensteobjekte anlegen	341
15.6.4	Maschinenobjekte anlegen	342
15.7	Weitere Werkzeuge	344

16	Active Directory mit Samba 4	345
16.1	Die Domäne einrichten	345
16.1.1	DNS verwalten	347
16.1.2	Ein erster Test	349
16.1.3	Ausfallsicherheit	350
16.2	Kerberos-Administration	351
16.2.1	Benutzerkonten und Gruppen verwalten	351
16.2.2	Principals verwalten	354
16.3	Sicherheitsrichtlinien	355
16.4	Domain Join und Keytab-Verwaltung	356
16.5	Fazit	357
17	Kerberos bei FreeIPA	359
17.1	FreeIPA im Überblick	359
17.1.1	IPA-Komponenten	360
17.1.2	Deployment-Szenario	361
17.2	Die Domäne einrichten	363
17.3	Verwaltungsaufgaben in der IPA-Domäne	367
17.4	Integration weiterer Linux-Systeme	371
17.5	Ausfallsicherheit	374
17.6	Fazit	375
18	Kerberos für Fortgeschrittene	377
18.1	Verteilte Kerberos-Umgebungen	377
18.1.1	Cross-Realm bei MIT Kerberos	378
18.1.2	Cross-Realm bei Heimdal	383
18.1.3	Cross-Realm bei Active Directory	386
18.1.4	Aufbau der Gesamtstruktur	390
18.2	Delegation für Fortgeschrittene	394
18.2.1	Vorbereitungen	395
18.2.2	Das Ok-As-Delegate Flag	396
18.2.3	kimpersonate	398
18.2.4	Constrained Delegation und Protocol Transition	400
18.3	PKINIT	402
18.3.1	Initiale Authentisierung mit Zertifikaten	403
18.3.2	PKINIT im Testnetz	404
18.3.3	Kerberos, PKINIT und Smartcards	409
18.3.4	Anonymes PKINIT	414
18.4	Zwei-Faktor-Authentisierung	414
18.4.1	OTP Tokens bei IPA	415
18.4.2	OTP und Passwort bei der Anmeldung	416
18.4.3	OTP und Passwort bei kinit	416

III	Integrierte Umgebungen	417
19	Grundlagen	421
19.1	Principals und Keytabs verwalten	421
19.1.1	Client-Principals anlegen	421
19.1.2	Funktionalität von Client-Principals prüfen	422
19.1.3	Dienste-Principals anlegen	423
19.1.4	Funktionalität von Dienste-Principals prüfen	423
19.1.5	Keytab-Dateien anlegen	424
19.1.6	Funktionalität von Keytab-Dateien prüfen	425
19.2	Zwischenstand	425
19.3	Die nativen Kerberos-Bibliotheken	426
19.4	GSS-API	426
19.5	SPNEGO	428
19.6	SSPI	428
19.7	SASL	429
19.7.1	Protokolle	429
19.7.2	Mechanismen	429
19.7.3	Konzepte	430
19.7.4	Cyrus SASL	431
19.8	Zusammenfassung	432
20	LDAP-Infrastruktur	433
20.1	LDAP im Überblick	433
20.1.1	Begriffe und Standards	433
20.1.2	Serverimplementierungen	435
20.1.3	Daten im LDAP	435
20.1.4	Verzeichnisoperationen	437
20.2	LDAP-Sicherheit	438
20.3	Kerberisierung bei Active Directory	439
20.4	Kerberisierung bei OpenLDAP	440
20.4.1	SASL-Konfiguration	441
20.4.2	Principal und Keytab	442
20.4.3	Identitätsmapping	443
20.5	Zusammenfassung	447
21	Clientanbindung	449
21.1	Windows-Clients in Active Directory	449
21.2	Linux-Clients in Active Directory	452
21.3	Der System Security Services Daemon	454
21.3.1	Einfache sssd-Konfiguration für Active Directory	455
21.3.2	Name Service Switch (NSS) mit sssd	457
21.3.3	Pluggable Authentication Modules (PAM) mit sssd	458

21.3.4	Erweiterte sssd-Konfiguration	461
21.4	Ausbau der Gesamtstruktur	466
21.4.1	LDAP-Referrals einrichten	466
21.4.2	Identitäts- und Autorisierungsdaten für Linux	467
21.5	Linux-Clients in der Gesamtinfrastruktur	473
21.5.1	Anbindung testen	473
21.5.2	Multi-Domänen-Anbindung konfigurieren und testen	475
21.5.3	Schattenobjekte für LDAP-Zugriff auf Active Directory	476
21.6	Zusammenfassung	478
22	Elementare Netzwerkdienste unter Unix und Linux	481
22.1	Kerberos mit OpenSSH	482
22.1.1	Vorbereitungen	482
22.1.2	Kerberisierte Secure-Shell-Sitzung	484
22.1.3	Tickets weiterleiten	486
22.1.4	Secure-Shell-Client unter Windows	486
22.1.5	OpenSSH ohne Kerberos Tickets	490
22.2	Remote-Dienste in verteilter Umgebung	491
22.2.1	Cross-Realm-Problematik	491
22.2.2	auth_to_local-Mappings	492
22.2.3	Heimdal	495
22.2.4	Cross-Realm-Anmeldung ohne Kerberos Tickets	495
23	Kerberisierte Dateisysteme	497
23.1	Server Message Block	497
23.1.1	SMB-Service unter Windows einrichten	498
23.1.2	Authentisierung bei SMB	500
23.1.3	SMB-Client unter Linux	501
23.1.4	SMB-Service unter Linux: Samba	502
23.1.5	ID Mapping	505
23.1.6	Heimatverzeichnisse für alle Windows-Nutzer	510
23.2	Network File System	511
23.2.1	Überblick	511
23.2.2	NFSv3 ohne Kerberos	512
23.2.3	NFSv3 und Sicherheit	514
23.2.4	NFSv4	515
23.2.5	Kerberisierter NFSv4-Service unter Linux	516
23.2.6	Den Server für Kerberos einrichten	520
23.2.7	Kerberisierter NFSv4-Client unter Linux	521
23.2.8	Den Client einrichten	522
23.2.9	NFSv4 und Sicherheit	523
23.2.10	NFSv4 in Cross-Realm-Umgebung	525
23.2.11	Abschlussarbeiten	525

23.3	Nichtinteraktiver Zugriff auf NFS-Verzeichnisse	526
23.3.1	Impersonifizierung über gssproxy einrichten	527
23.3.2	Impersonifizierung testen	527
23.4	Zusammenfassung	528
24	Single Sign-on für Webdienste	529
24.1	Kerberos und das HTTP-Protokoll	529
24.1.1	Das World Wide Web	529
24.1.2	Authentisierung im HTTP-Protokoll	530
24.1.3	Negotiate (SPNEGO)	531
24.2	Den Apache-Server konfigurieren	531
24.2.1	Voraussetzungen	532
24.2.2	Principals und Keytab-Einträge	533
24.2.3	mod_auth_gssapi konfigurieren	535
24.3	Browserkonfiguration	537
24.3.1	Vertrauenswürdige Seiten konfigurieren	537
24.3.2	Zugriff testen	539
24.3.3	Delegation konfigurieren	541
24.3.4	Delegation testen	542
24.4	Autorisierungsdaten und Ticket-Größe	545
24.5	Autorisierung über LDAP	546
24.6	Kerberos und Web-SSO	549
24.6.1	Keycloak installieren	549
24.6.2	Keycloak kerberisieren	552
24.6.3	Account-Konsole als Test	553
24.6.4	Erweiterungsmöglichkeiten	554
24.7	Kerberos-Authentisierung im Web-Proxy	554
24.7.1	Den Squid-Proxy vorbereiten	555
24.7.2	Kerberos-Principal für Squid	555
24.7.3	Squid-Anmeldung konfigurieren	556
24.7.4	Browserkonfiguration für Proxy-Authentisierung	557
24.8	Zusammenfassung	558

IV Anhang 559

A	Schnelleinstieg in LDAP	561
A.1	LDIF	561
A.1.1	Das LDAP-Datenmodell	561
A.1.2	LDIF-Repräsentation von LDAP-Daten	562
A.1.3	Änderungen mit LDIF	563
A.2	OpenLDAP-Tools	565
A.2.1	Suchen mit ldapsearch	565

A.2.2	Authentisierung	566
A.2.3	Weitere OpenLDAP-Kommandos	568
A.3	Grafische LDAP-Werkzeuge	568
B	Konfiguration der Betriebssysteme	571
B.1	Netzwerkparameter	571
B.2	CentOS 8	571
B.3	Windows Server 2019	573
B.4	Windows 10	574
C	Softwareinstallationen	575
C.1	Vorbemerkungen	575
C.2	MIT Kerberos	576
C.3	Heimdal	577
C.4	k5start	578
C.5	mktutil	578
C.6	Samba	579
	Literaturverzeichnis	581
	Index	587