

Inhaltsverzeichnis

Vorwort	13
Kapitel 1 Die Bedeutung der Registry	15
1.1 Die Bedeutung der Registry für den Windows-Rechner	16
1.2 Wann sind manuelle Eingriffe in die Registry nötig?	17
1.3 Ist es gefährlich, in der Registry zu arbeiten?	18
1.4 Fallbezogenes, praxisnahes Wissen	18
1.5 Datenbank für die Registry: <i>RegCheck</i>	19
1.5.1 In diesem Buch: CD-ROM mit <i>RegCheck</i>	19
1.5.2 Die Bedeutung der Expertensysteme	19
1.5.3 <i>RegCheck</i> : Hart an den Fakten	21
1.5.4 <i>RegCheck</i> : Registry-Abgleich mit Referenzen	22
1.5.5 <i>RegCheck</i> : Völlig neue Möglichkeiten	23
1.6 Die Registry im betrieblichen Ablauf	24
1.6.1 Registry und Revision	24
1.6.2 Registry und externe Dienstleister	26
1.6.3 Registry und Techniker/Administratoren	27
1.7 Die Microsoft-Bordmittel	27
1.7.1 RegEdit4, RegEdit5, RegEdit32, REG.EXE	27
1.7.2 RegEdit → .REG → RegCheck → .REG	28
1.8 Software von Drittherstellern	28
Kapitel 2 Die Entstehung der Registry über verschiedene Windows-Versionen hinweg	31
2.1 Vorgeschichte	32
2.2 Windows 3.0: Einstellungen via .INI	32
2.3 Windows 3.1: Die erste Registry mit REG.DAT	35
2.4 Windows 95, 98	37
2.5 Windows NT 3.1, 3.5, 3.51: Die Registry wird erwachsen	38
2.6 Windows NT 4	39

2.7	Windows 2000	40
2.8	WinNT4 vs. Win2000 (Server): Schlüssel und Werte mit gleichen bzw. verschiedenen Funktionen	41
Kapitel 3	Quellen zur Registry	45
3.1	Microsoft – www.microsoft.com	46
3.1.1	Windows Resource Kit	46
3.1.2	Internet-Recherche	46
3.1.3	Microsoft KnowledgeBase/Q-Artikel	49
3.1.4	TechNet-CD	49
3.1.5	Microsoft-Literatur	49
3.1.6	Der aktuelle Stand der Registry	49
3.2	Novell – www.novell.com	50
3.3	IBM – www.ibm.com	51
3.4	SysInternals – www.sysinternals.com	53
3.5	Winternals – www.winternals.com	53
3.6	Tools4NT – www.tools4nt.com	53
3.7	Beverly Hills Software – www.bhs.com	53
3.8	WinGuides – www.winguides.com	54
3.9	ICARUS – www.ica-r-us.de	54
3.10	Synapse: Networks – www.synapse.de	54
Kapitel 4	Werkzeuge für die Registry	57
4.1	RegEdit und .REG-Dateien	58
4.1.1	Was ist RegEdit?	58
4.1.2	Was wird von RegEdit sichtbar gemacht?	58
4.1.3	RegEdit und .REG-Dateien	60
4.2	PolEdit und .ADM-Dateien	61
4.2.1	PolEdit seit Windows NT 3.1	61
4.2.2	PolEdit, ADS und GPOs unter Windows 2000	61
4.2.3	System Policy = Systemrichtlinie	62
4.2.4	.POL-Dateien	62
4.2.5	.ADM-Dateien/Scripts	63
4.2.6	Systemrichtlinien für Rechner und für Benutzer	63
4.2.7	Systemrichtlinien und die Registry	63
4.2.8	Beispiel einer .ADM-Datei	64
4.2.9	Hilfe zum Erstellen der .ADM-Dateien	68

4.3	Microsoft Windows Resource Kits	68
4.3.1	Windows NT 4 Resource Kit	68
4.3.2	Windows 2000 Resource Kit	70
4.4	Weitere Registry-Tools von Microsoft	71
4.4.1	Microsoft: RegClean	71
4.4.2	Microsoft: WinDiff	71
4.5	Tools für die Registry von Drittherstellern	71
4.5.1	RegMon – Registry Monitor	72
4.5.2	Aelita Software: ERDisk, MultiReg, RegAdmin	72
4.5.3	Adkins Resource: Hyena	73
4.5.4	SystemTools: Security Explorer	73
4.5.5	SomarSoft: DumpReg, DumpSec, DumpEvt	73
4.5.6	SomarSoft: DumpACL (jetzt: DumpSec)	74
4.5.7	McAfee: Uninstaller	74
4.5.8	Norton Utilities: WinDoctor	74
4.5.9	Hoek Software: RegSearch	74
4.5.10	SmartLine: Active Registry Monitor	74
4.5.11	ProStream: RegWeb	75
4.5.12	Imagine LAN: RegSafe, ConfigSafe, RecoverySafe	75
4.5.13	DC Software: RegEditX	75
4.5.14	Nickles: RegView	76
4.5.15	Synapse:Networks: RegCheck	76
4.5.16	Weitere Fundstellen im Internet	76
Kapitel 5	Der Aufbau der Registry	77
5.1	Die Position im Dateisystem	79
5.1.1	Windows-Systemverzeichnisse mit Registry-Daten	79
5.1.2	Verzeichnisnamen in Englisch bzw. Deutsch	80
5.1.3	Die hinter der Registry liegenden Dateien	81
5.2	Registry-Hives	84
5.2.1	Die Trennung von Hardware, Software, User	84
5.2.2	Übersicht der Hauptschlüssel: HKEY_...	85
5.2.3	HKEY_LOCAL_MACHINE (HKLM)	86
5.2.4	HKEY_CURRENT_CONFIG (HKCC)	95
5.2.5	HKEY_USERS (HKU)	96
5.2.6	HKEY_CURRENT_USER (HKCU)	99
5.2.7	HKEY_CLASSES_ROOT (HKCR)	100

5.2.8	HKEY_PERFORMANCE_DATA (HKPD)	111
5.3	Die innere Struktur der Registry	111
5.3.1	Die Begriffe Hive, Key, Subkey, Entry, Value, etc.	111
5.3.2	Die Hierarchie der Registry	112
5.3.3	Hive Key – Hauptschlüssel	112
5.3.4	SubKey – Unterschlüssel/Pfade und ihre Darstellung	112
5.3.5	Entry – Name des Eintrags	116
5.3.6	Value – Wert des Eintrags	117
5.3.7	Data Type – Datentyp des Wertes	117
5.4	Datentypen: REG_BINARY, REG_SZ etc.	118
5.4.1	REG_NONE =hex(0)	122
5.4.2	REG_DWORD =dword:00000000	122
5.4.3	REG_DWORD_LITTLE_ENDIAN =hex(4)	126
5.4.4	REG_DWORD_BIG_ENDIAN =hex(5)	127
5.4.5	REG_SZ ="..."	127
5.4.6	REG_MULTI_SZ =hex(7)	128
5.4.7	REG_EXPAND_SZ =hex(2)	129
5.4.8	REG_BINARY =hex:...	130
5.4.9	REG_RESOURCE_LIST =hex(8)	131
5.4.10	REG_FULL_RESOURCE_DESCRIPTOR =hex(9)	133
5.4.11	REG_RESOURCE_REQUIREMENTS_LIST =hex(a)	133
5.4.12	REG_LINK = Registry-Verweis	134
5.5	Verweise auf andere Registry-Werte	135
5.5.1	Unterschied zwischen Verweisen und Links	135
5.5.2	RegLocation: Registry-Pfad mit Service-Variable	136
5.5.3	KeyType: Registry-Datentyp	137
5.5.4	Beispiel: DHCP Options	137
5.6	SID – Security ID	147
5.7	GUID – Globally Unique ID	153
5.8	Die Konfigurationssätze	153
5.8.1	Die Komponenten eines Konfigurationssatzes:	153
5.8.2	Control	153
5.8.3	Enum	161
5.8.4	Hardwareprofile	165
5.8.5	Services	166
5.9	Die Registry beim Bootvorgang	169
5.9.1	Hardwareerkennung: ntdetect	169

5.9.2	Das Laden der Treiber	170
5.9.3	Dynamische Daten und die Registry	171
5.9.4	Benutzerprofile/Benutzereinstellungen	171
5.9.5	System Policy/Group Policy	172
5.10	OLE, COM, ActiveX und Class IDs (CIDs)	173
5.11	Dateiendungen: .TXT etc.	174
5.12	Registry-Werte von Anwendungssoftware	177
Kapitel 6	Windows 2000: Neuerungen, Abweichungen	179
6.1	Veränderte Zeichensatz-Tabellen	180
6.1.1	ANSI vs. Unicode	180
6.1.2	RegEdit4 vs. RegEdit5	180
6.1.3	Vermeintliche Leerzeichen, die keine sind	181
6.2	Veränderter Auftritt von Hardware-Ressourcen in der Registry	181
6.3	GUIDs: Globally Unique IDs	181
6.3.1	GUIDs am Beispiel von Netzwerk-Adaptern	182
6.3.2	GUIDs und die daraus folgenden Schwierigkeiten	201
6.3.3	Zusammenfassung	211
6.4	HKEY_CURRENT_USER	212
6.4.1	Erweiterter Umfang bei Win2000	212
6.4.2	Veränderte Pfade bzw. Standorte von Werten	212
6.4.3	Neue Schlüssel für neue Funktionen	212
6.5	Windows XP: Rücknahme von Win2000-Neuerungen?	212
Kapitel 7	Sicherheit und Netzwerk	215
7.1	Sicherheit: Die Zugriffsrechte der Registry	216
7.1.1	Registry: Funktionen und Rechte	216
7.1.2	Schlüsseleigentümer (Owner)	217
7.1.3	Zugriffsprotokoll (Auditing/Audit Trail)	217
7.1.4	SYSKEY: Verschlüsselung von SAM und SECURITY	217
7.2	Der Fernzugriff via Netzwerk	218
7.3	SecurePipeServers\WinReg	218
7.4	DisableRegistryTools	219

Kapitel 8	Sicherung der Registry	221
8.1	Booten mit anderen Betriebssystemen	222
8.2	Booten im DOS-Modus	223
8.3	ERD – Emergency Repair Disk	223
8.4	Windows 2000 Recovery Console	224
8.5	ERD und Hives in RegEdit32	225
8.5.1	Windows NT 4.0 und RegEdit32	225
8.5.2	Windows 2000 und RegEdit32	225
8.6	Sicherung in Textdateien: .REG	225
8.6.1	RegEdit32	226
8.6.2	RegEdit4, RegEdit5	227
8.7	Backup der Registry-Hive-Dateien	231
8.7.1	Backup-Software von Drittherstellern	231
8.7.2	Das Backup-Programm von Windows NT	231
8.7.3	Das Backup-Programm von Windows 2000	232
8.7.4	Sicherung mit RegBack	232
8.7.5	Rückschreibung mit RegRest	233
Kapitel 9	Das Editieren der Registry	235
9.1	Warnung vor Fehlern!	236
9.2	DisableRegistryTools	237
9.3	RegEdit-Versionen und ihre Unterschiede	237
9.3.1	Unterschiede (Übersicht)	237
9.3.2	Die verschiedenen .REG-Textformate	238
9.3.3	Werte und Datentypen (Unterschiede)	239
9.3.4	Zugriffsrechte in der Registry/RegEdit32	242
9.4	Registry-Editoren von Drittherstellern	246
9.5	RegCheck vs. RegEdit	246
Kapitel 10	Das Registry-Expertensystem <i>RegCheck</i>	249
10.1	Die Hauptfunktionen von <i>RegCheck</i>	250
10.2	Die <i>RegCheck</i> -Funktionen im Programm	251
10.3	Daten aus einer .REG-Datei in <i>RegCheck</i> einlesen	254
10.3.1	Das Setzen des Import-Filters	255
10.3.2	Auswahl der .REG-Datei und Import-Start	257
10.4	Die [DB]-Import-Datenbank	263

10.4.1	Der Tabellenaufbau	263
10.4.2	Tabellenstruktur ohne Baumdarstellung	263
10.4.3	Tabellenfenster vergrößern/verkleinern	264
10.4.4	Registry-Anzeige ein-/ausschalten	267
10.4.5	Tabellenverknüpfung (Hierarchie) ein-/ausschalten	268
10.4.6	Sortieren von Registry-Tabellen	270
10.4.7	Setzen der mächtigen Tabellenfilter	273
10.4.8	Ausführliche Anzeige eines Registry-Wertes	276
10.5	Die [TT]-Referenzdatenbank	277
10.5.1	Die Tabellenstruktur der Referenzdatenbank	277
10.5.2	Die Tabelle der Referenz-Bibliotheken	278
10.5.3	Weitergabe von Referenz-Bibliotheken	280
10.5.4	Exportieren von Referenzdaten	281
10.5.5	Importieren von Referenzdaten	284
10.5.6	Übergabe von Registry-Daten aus der [DB]-Import-Datenbank an die [TT]-Referenzdatenbank	289
10.5.7	Manuelle Eingabe von Registry-Werten	294
10.5.8	Eingaben in die Wissensdatenbank (Memofelder, Textfelder)	296
10.5.9	Variablen im Registry-Pfad: SID, GUID etc.	298
10.5.10	Kompatibilitäts-Abgleich zwischen Windows NT 4 und Windows 2000	300
10.6	Registry Check: Abgleich zwischen [DB]-Import-Datenbank und [TT]-Referenzdatenbank	301
10.7	Die Export-Tabelle (Vorschlagsliste): Die Ausgabe einer neuen .REG-Datei	305
10.7.1	Automatisches Erzeugen der Vorschlagsliste nach einem Registry-Abgleich	305
10.7.2	Die Vorschlagsliste in der Export-Tabelle	307
10.7.3	Manuelle Auswahl der Referenz-Bibliothek	308
10.7.4	Eindeutigkeit der exportierten Registry-Werte	308
10.7.5	Automatischer Test mit Ansicht und ggf. Korrektur	309
10.7.6	Registry-Export in eine neue .REG-Datei	309
10.8	WWW: Die Publikation von Referenzdaten als HTML-Projekt	312
10.8.1	Geschlossenes HTML-Projekt	312
10.8.2	Halbautomatisches Erzeugen von HTML-Code	312
10.8.3	Die HTML-Metatags	313
10.8.4	Hintergrundfarbe bzw. -Grafik/Textgröße	313
10.8.5	Einführungs- oder Begrüßungstext	313

10.8.6	Absender- oder Urheberkennung	315
10.8.7	Export-Filter in der [TT]-Referenzdatenbank	315
10.8.8	Wahl des Ausgabeverzeichnis	316
10.8.9	Letzte Prüfung – und START	316
10.8.10	Das Ergebnis auf der Festplatte	317
10.8.11	Das Ergebnis im Internet: WWW	318
10.9	<i>RegCheck</i> : Installation der Software von CD-ROM	320
10.10	<i>RegCheck</i> : Update auf die aktuelle Programmversion	321
Kapitel 11	Migration von Windows NT 4 zu Windows 2000	323
11.1	Dokumentation der Win2000-Registry	324
11.2	Archivierung der WinNT4-Registry	324
11.3	Archivierung der Win2000-Registry	324
11.4	Voraussetzungen für den Abgleich zwischen WinNT4-Registry und Win2000-Registry	324
11.5	Vergleiche der Registry zwischen Windows NT 4 und Windows 2000	325
11.5.1	Direkter Vergleich trotz starker Registry-Unterschiede	325
11.5.2	Zentraler Punkt: Netzwerk mit TCP/IP	326
11.5.3	Die Bedeutung von DHCP und Dynamic DNS	326
11.5.4	Windows 2000-Arbeitsrechner	327
11.5.5	Windows 2000 Server	327
11.6	Erfahrungsaustausch zwischen Lesern und <i>RegCheck</i> -Anwendern	327
Anhang A	TCP/IP-Parameter von Windows 2000	333
Anhang B	DNS-Parameter von Windows 2000	413
Anhang C	Installation von <i>RegCheck</i>	463
C.1	Systemvoraussetzungen	463
C.2	Installation und Setup-Dialoge	464
C.3	Erster Start von <i>RegCheck</i>	467
C.4	Das Laden von <i>RegCheck</i>	470
C.5	Die <i>RegCheck</i> -Lizenzierung	471
	Stichwortverzeichnis	475