FAQ
Die Windows-Registry

Antworten auf die häufigsten Fragen

Von Hajo Schulz und Axel Vahldiek

Sinn und Zweck

? Was ist überhaupt die Registry? Wozu ist sie da?

! Die Registry – oder auf Deutsch Registrierdatenbank – ist die zentrale Instanz, in der Windows seine Einstellungen und andere Konfigurationsdaten speichert. Auch den Entwicklern von Anwendungen empfiehlt Microsoft, solche Daten hier abzulegen.

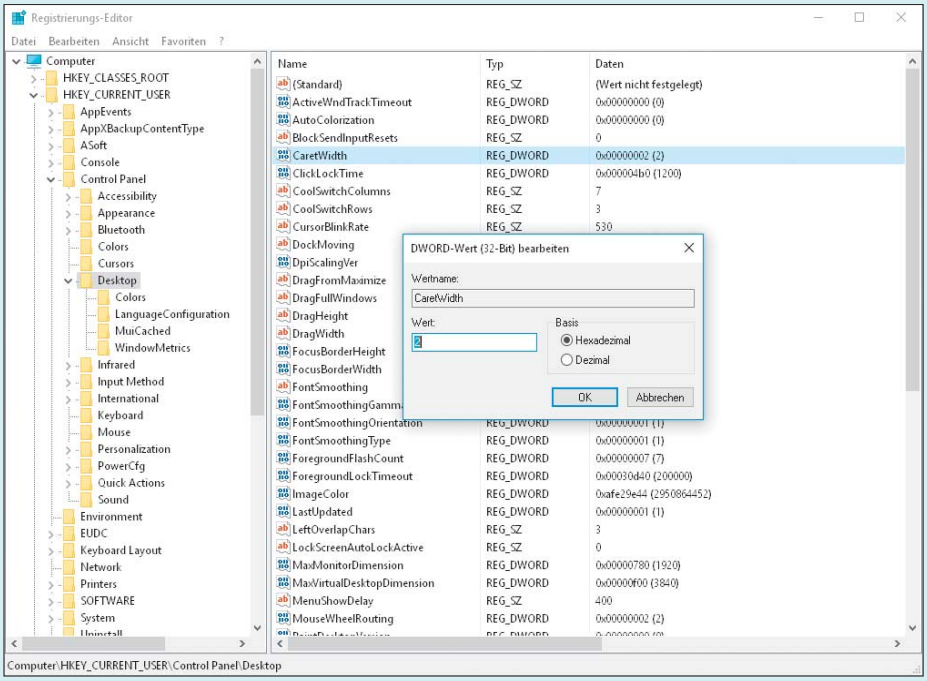
In den allerersten Windows-Versionen, in denen es die Registry noch nicht gab, kochte jeder Software-Hersteller sein eigenes Süppchen und speicherte solche Informationen in INI-Dateien oder eigenen Binärformaten, und auch der Speicherort war nicht standardisiert. Mit Windows NT und seinem ausgefeilten Konzept der Rechte-Zuweisung für alle möglichen Objekte reichte diese unstrukturierte Speicherung nicht mehr aus. Microsoft propagierte fortan die Registry, die schon seit Windows 3.1 existierte und als Registratur für OLE-Komponenten diente, als zentrale, universelle Konfigurationsdatenbank.

In letzter Zeit weist der Trend eher wieder in die entgegengesetzte Richtung: Moderne Programme und Apps speichern ihre Konfiguration mehr und mehr in eigenen XML- oder JSON-Dateien. Um Einstellungen für Windows selbst und die Mehrzahl althergebrachter Anwendungen zu überprüfen und gegebenenfalls zu korrigieren, ist die Registry aber immer noch der wichtigste Ort.

Reinschauen

? Mit welchem Programm kann ich mir den Inhalt der Registry ansehen? Wie ändere ich dort Einstellungen?

! Es gibt mehrere Bordmittel, mit denen man sich Zugriff auf die in der Registry gespeicherten Daten verschaffen kann. Das wahrscheinlich populärste ist das Programm regedit aus dem Windows-Ordner. Dieser „Registrierungs-Editor“ taucht im Startmenü nicht auf, lässt sich aber einfach starten, indem man in den „Ausführen“-Dialog (Tastenkombination Win+R) `regedit` eintippt. Alternativ kann man diesen Namen auch in das Suchfeld des Startmenüs beziehungsweise von Cortana eingeben und mit Enter bestätigen.



Die Daten in der Registry sind ähnlich wie die Dateien und Ordner auf der Festplatte baumartig organisiert. Deshalb sieht der Registry-Editor auf den ersten Blick auch fast wie ein Explorer aus.

Der Registry-Editor sieht auf den ersten Blick einem Explorer-Fenster nicht unähnlich und lässt sich auch fast so bedienen: Auf der linken Seite listet er baumartig strukturiert die vorhandenen „Schlüssel“ (dazu gleich mehr); klickt man einen an, erscheinen rechts die dazugehörigen Einträge, die man per Doppelklick oder Kontextmenü bearbeiten kann.

Eher für Skript- und Batch-Programmierer ist das Kommandozeilenprogramm `reg` gedacht: Mit ihm kann man die Registry in der Eingabeaufforderung auslesen und Inhalte ändern. Näheres zu seinen Optionen verrät der Aufruf `reg /?`.

Auch in der Windows PowerShell gibt es Befehle zum Zugriff auf die Registry: Hier erscheint sie als ein Satz virtueller Laufwerke, in denen man wie durch die Ordner einer Festplatte navigieren kann; Schlüssel spielen die Rolle von Dateien und Ordnern und lassen sich mit den dafür üblichen Befehlen anlegen, löschen, kopieren, umbenennen und so weiter. Einstiege in die zuständige Dokumentation liefern die Aufrufe `Get-Help Registry` und `Get-Help about_Providers`.

Was ist wo?

? Schlüssel, Einträge, `HKEY_CLASSES_ROOT`, `HKEY_LOCAL_MACHINE` – wie soll man sich denn da zurechtfinden?

! Die Daten sind in der Registry hierarchisch organisiert. Diese Ordnung gibt auch der Registry-Editor wieder: In der linken Baumansicht zeigt er die **Schlüssel**. Jeder Schlüssel kann einerseits weitere Schlüssel enthalten – im Registry-Editor durch aufklappbare Untereinträge im Baum dargestellt. Zudem enthalten Schlüssel beliebig viele **Werte** – die Ein-

träge auf der rechten Seite im regedit. Jeder Wert besitzt einen Namen und einen Inhalt. Welcher Art der Inhalt ist, wird durch einen von sechs möglichen Datentypen bestimmt. Die gebräuchlichsten sind Zeichenfolgen, DWORD für Ganzzahlen zwischen 0 und 4 294 967 295 sowie Binärdaten für beliebige Inhalte, die die zuständige Anwendung interpretieren muss.

Es gibt fünf Einstiege in die Schlüsselhierarchie: Unter HKEY_LOCAL_MACHINE (kurz HKLM) finden sich Daten, die systemweit gelten, unter HKEY_CURRENT_USER (HKCU) solche, die nur das aktuelle Benutzerkonto betreffen. Je nach Geltungsbereich legen Anwendungen ihre Konfigurationsdaten üblicherweise in einem dieser Zweige ab, und zwar in einem Unterschlüssel nach dem Muster Software\Hersteller\Programmname.

In den Unterschlüsseln von HKEY_CLASSES_ROOT (HKCR) speichert Windows Informationen über Dateitypen und COM-Klassen, also etwa was passiert, wenn Sie eine bestimmte Datei im Explorer doppelklicken, oder was nötig ist, um eine Excel-Tabelle in ein Word-Dokument einzubetten. Die Daten unter HKCR stammen in Wahrheit aus den Schlüsseln unter HKLM\Software\Classes und HKCU\Software\Classes; existieren in beiden Ästen gleichnamige Werte, gewinnt HKCU.

Unter HKEY_USERS (abgekürzt HKU) gibt es für jedes aktuell angemeldete Benutzerkonto einen Schlüssel, der dessen HKCU-Zweig entspricht. Dazu gehören auch die Systemkonten „Lokales System“ (S-1-5-18 und .DEFAULT), „Lokaler Dienst“ (S-1-5-19) und „Netzwerkdienst“ (S-1-5-20). Der Schlüssel HKEY_CURRENT_CONFIG (HKCC) ist in Zeiten von Plug&Play-Hardware ziemlich unwichtig geworden; er ist auch nur eine Abkürzung zu HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\Current.

Speicherort

? Wo genau liegt die Registry auf der Festplatte?

! Die Registry verteilt sich auf mehrere sogenannte Hive-Dateien. Wo genau die jeweils liegen, lässt sich in der Registry selbst nachschauen, und zwar unter HKLM\SYSTEM\CurrentControlSet\Control\hivelist. Normalerweise residiert der benutzerspezifische Teil der Registry (HKCU) als ntuser.dat im Benutzerprofil unter c:\users*Kontoname*, während der systemspezifische Teil (HKLM) unter c:\windows\system32\config liegt. Dort ist er wiederum auf mehrere Dateien aufgeteilt (siehe Tabelle). Eine Ausnahme ist der Schlüssel HKLM\HARDWARE: Er enthält Informationen über die gerade angeschlossene Hardware und wird dynamisch zur Laufzeit erzeugt, hinter ihm steckt also keine Datei.

Blick auf die Hive-Dateien

? Ich möchte mir selbst einen Eindruck vom Inhalt des Ordners c:\windows\system32\config verschaffen.

! Das ist nicht ganz trivial. Das fängt schon damit an, dass der Explorer standardmäßig versteckte und Systemdateien ausblendet. Ändern Sie das in den Ordneroptionen in der Systemsteuerung (heißen bei Windows 10 „Explorer-Optionen“). Entfernen Sie unter Ansicht die Häkchen vor „Erweiterungen bei bekannten Dateien ausblenden“ sowie bei „Geschützte Systemdateien ausblenden“ und bestätigen Sie die Nachfrage. Scrollen Sie weiter runter und stellen Sie unter „Versteckte Dateien und Ordner“ um auf „Ausgeblendete Dateien, Ordner und Laufwerke anzeigen“.

Im Prinzip können Sie nun den Inhalt des Ordners config einsehen, doch geht das nur als Administrator. Der Explorer läuft allerdings auch dann nur mit eingeschränkten Rechten, wenn das von Ihnen genutzte Konto Mitglied der Gruppe der Administratoren ist. Es hilft auch nicht, den Explorer per Rechtsklick „Als Administrator“ auszuführen – da der Explorer auch als Shell läuft, würde einfach nur ein weiteres Fenster aufgehen, welches wieder nur mit eingeschränkten Rechten läuft.

Sie könnten die Rechte am Ordner config anpassen, um mit eingeschränkten Rechten hineinsehen zu können. Weniger Gefahr von Nebenwirkungen birgt es jedoch, einen alternativen Dateimanager wie Total- oder FreeCommander zu benutzen und den mit Administratorrechten zu starten. Sollten Sie so etwas nicht zur Hand haben, geht es auch ohne: Starten Sie den Editor Notepad aus dem Startmenü via Kontextmenü „Als Administrator“. Drücken Sie Strg+O für den „Öffnen“-Dialog und stellen Sie die Ansicht unten rechts von „Textdateien (*.txt)“ auf „Alle Dateien (*.*)“ um. Nun können Sie sich im Öffnen-Dialog zum Ordner config durchhangeln und hineinsehen.

Dateien der Registry-Hives

Registry-Schlüssel	Datei	Zweck
HKEY_CURRENT_USER	c:\users*Kontoname*\ntuser.dat	kontospezifische Einstellungen
HKLM\components	c:\windows\system32\config\components	Zustand von Windows-Funktionen und -Updates
HKLM\sam	c:\windows\system32\config\sam	Security Accounts Manager, enthält unter anderem Anmeldenamen und Hashes der Kennwörter
HKLM\security	c:\windows\system32\config\security	Sicherheitsrichtlinien und Benutzerrechte
HKLM\software	c:\windows\system32\config\software	systemweit geltende Einstellungen für Windows und Anwendungen
HKLM\system	c:\windows\system32\config\system	Windows-Einstellungen, die bereits während des Hochfahrens benötigt werden, etwa über Treiber und Dienste
HKU\.default	c:\windows\system32\config\default	kontospezifische Einstellungen für das Konto „Lokales System“ (local system)
HKU\S-1-5-19	c:\windows\system32\ServiceProfiles\LocalService\Ntuser.dat	kontospezifische Einstellungen für das Konto „Lokaler Dienst“ (local service)
HKU\S-1-5-20	c:\windows\system32\ServiceProfiles\NetworkService\Ntuser.dat	kontospezifische Einstellungen für das Konto „Netzwerkdienst“ (network service)

Registry-Backup

? Wie sichere ich die Registry am besten? Kann ich die Hive-Dateien einfach kopieren?

! Das Sichern der einzelnen Dateien hilft nicht. Die Informationen in der Registry beziehen sich auf Windows und die installierten Anwendungen, daher sollte alles stets auf demselben Stand sein, um etwa nach Updates Inkonsistenzen zu vermeiden. Sichern Sie daher nicht die Hive-Dateien allein, sondern die komplette Windows-Partition, und zwar mit einem Imager. Ab Windows 8.1 empfehlen wir c't-WIMage dafür [1] (bitte auch [2] beachten). Wer noch Windows 7 benutzt, kann zu Drive Snapshot greifen – eine 1-Jahres-Vollversion ist Bestandteil des c't-Notfall-Windows [3].

Sicherheitskopie

? Ich möchte nur einen einzelnen Schlüssel ändern und davon vorher ein Backup erzeugen. Geht das nicht mit weniger Aufwand als mit einem Image?

! Ja, Sie können Schlüssel auch einzeln sichern – und sollten sich angewöhnen, das immer zu tun, bevor Sie Einstellungen direkt in der Registry ändern. Der zuständige Befehl steckt beim Registry-Editor im Datei-Menü und heißt Exportieren. Bevor Sie ihn aufrufen, müssen Sie den zu speichernden Schlüssel in der Baumansicht auswählen – wenn Sie vorhaben, Schlüssel zu löschen, setzen Sie sicherheitshalber eine Etage höher an als direkt bei diesem Schlüssel. Komplette Wurzelschlüssel wie HKCU oder HKCR auf diese Weise zu sichern, ergibt aber wenig Sinn: Zum einen würde die entstehende Datei sehr groß werden, zum zweiten ändern sich zahlreiche Registry-Einträge recht oft, sodass Sie beim großflächigen Zurückimportieren womöglich irgendeine Systemfunktion aus dem Tritt bringen.

Bei den .reg-Dateien, die der Exportieren-Befehl erzeugt, handelt es sich um gewöhnliche Textdateien, die Sie mit einem beliebigen Editor wie Notepad bearbeiten können. Aber Vorsicht: Wie in der Registry selbst können unbedachte Änderungen hier weit reichende Folgen haben.

Um eine .reg-Datei wieder in die Registry einzulesen, verwenden Sie den Befehl Datei/Importieren im Registry-Editor. Alternativ können Sie die Datei auch einfach im Explorer doppelklicken.

Aufräumen

? Man liest ja immer wieder, dass eine volle Registry Windows ausbremst. Welches Tool können Sie mir empfehlen, um sie aufzuräumen?

! Gar keines. Eine große Registry hat unseren Tests zufolge kaum mess-, geschweige denn spürbare Auswirkungen auf die Systemgeschwindigkeit. Das ist auch logisch, denn Windows und Anwendungen lesen immer nur die Einträge, die sie kennen. Die paar Bytes, die unbenutzte Einträge auf der Festplatte belegen, sind selbst bei einer knapp bemessenen SSD vernachlässigbar. Die Gefahr, dass so ein angeblicher Windows-Beschleuniger Einträge löscht, die eigentlich noch gebraucht werden, ist unserer Erfahrung nach jedenfalls deutlich größer als die Aussicht auf eine tatsächliche Geschwindigkeitssteigerung.

Schreibfehler

? Bei dem Versuch, bestimmte Registry-Werte zu ändern oder zu löschen, meldet der Registry-Editor immer mal wieder, dass er die Änderung nicht schreiben konnte. Was kann ich dagegen tun?

! Wahrscheinlich fehlt Ihnen die Berechtigung, die gewünschte Änderung durchzuführen. Registry-Schlüssel tragen ähnlich wie Dateien und Ordner auf NTFS-Laufwerken Sicherheitsinformationen, die festlegen, welcher Benutzer hier lesen, schreiben, löschen und so weiter darf. Standard-Benutzer haben Schreibzugriff nur auf Unterschlüssel von HKCU, also die Daten, die zu ihrem Benutzerprofil gehören.

Nur wenn der Registry-Editor von einem Mitglied der Benutzergruppe der Administratoren gestartet wird, bittet er per UAC-Abfrage um volle Rechte. Dann kann der Benutzer fast überall lesen und schreiben. Ausnahme sind die Unterschlüssel von HKLM\SAM, in denen unter anderem die Passwort-Hashes aller Benutzerkonten gespeichert sind: Sie bleiben selbst Administratoren verborgen.

Entsprechende eigene Berechtigungen vorausgesetzt können Sie die Rechte an Registry-Schlüsseln notfalls auch ändern; im Registry-Editor dient dazu der Befehl „Berechtigungen“ aus dem Kontextmenü von Schlüsseln. Der daraufhin erscheinende Dialog funktioniert genauso wie die Seite „Sicherheit“ auf dem Eigenschaften-Dialog von Dateien und Ordnern im Explorer. Ähnlich wie im Dateisystem ist es aber auch in der Registry keine gute Idee, Rechte zu lax zu vergeben – wir können eigentlich nur davor warnen, hier überhaupt Hand anzulegen: Die nächste Malware wartet schon darauf, die Löcher auszunutzen, die man durch unbedachte Änderungen aufreißt.

HKCU unter HKU suchen

? Der Schlüssel `HKCU` ist ja bloß ein Spiegel eines der Schlüssel unter `HKU`. Doch da derzeit mehrere Konten angemeldet sind, finde ich dort viele Unterschlüssel. Wie bekomme ich heraus, welcher zu meinem Konto gehört?

! Mit einem Kniff: Erzeugen Sie direkt unter `HKCU` einfach einen Zeichenfolgenwert namens `Werbinich`, dem Sie als Inhalt den Namen des von Ihnen gerade benutzten Kontos zuweisen. Anschließend klicken Sie die Schlüssel unter `HKU` so lange durch, bis Sie die Zeichenfolge dort wiedergefunden haben – dieser Schlüssel ist dann der Ihres Kontos. Wenn Sie das einmal mit allen Benutzerkonten machen, wird das Identifizieren künftig einfach.

Sie brauchen beim Anlegen so eines für Windows nutzlosen Schlüssels übrigens keine Angst vor irgendwelchen Schäden zu haben. Windows liest immer nur das aus, was es auch kennt – alles andere ignoriert es einfach.

Offline bearbeiten

? Ich will die Registry einer Windows-Installation bearbeiten, die derzeit gar nicht läuft.

! Dann brauchen Sie dafür entweder ein parallel installiertes Windows oder eines, das von einem externen Medium bootet, etwa unser c't-Notfall-Windows. Booten Sie dieses Windows und starten Sie Regedit wie gewohnt. Markieren Sie nun den Schlüssel `HKLM` und klicken Sie dann im Menü auf „Datei/Struktur laden“ (ist der Menüpunkt ausgegraut, wurde `HKLM` nicht markiert). Es erscheint ein „Öffnen“-Dialog, in dem Sie zunächst die Systempartition der Festplatte mit der gewünschten Windows-Installation suchen müssen – sie trägt hier in der Regel einen anderen Buchstaben als C.

Nun können Sie sich zur Datei mit dem passenden Registry-Hive durchhangeln, beispielsweise „Software“. Der Registry-Editor fragt nach einem Namen – vergeben Sie einen beliebigen wie „offline“. Anschließend finden Sie den nun eingehängten Registry-Hive unter `HKLM\offline`. Bearbeiten Sie ihn wie gewünscht. Wenn Sie damit fertig sind, vergessen Sie bitte nicht, ihn wieder freizugeben. Dazu markieren Sie `HKLM\offline` und klicken unter „Datei“ auf „Struktur entfernen“.

Vergleichen

? Ich suche eine möglichst einfache Methode, um Registry-Schlüssel von verschiedenen Windows-Installationen zu vergleichen.

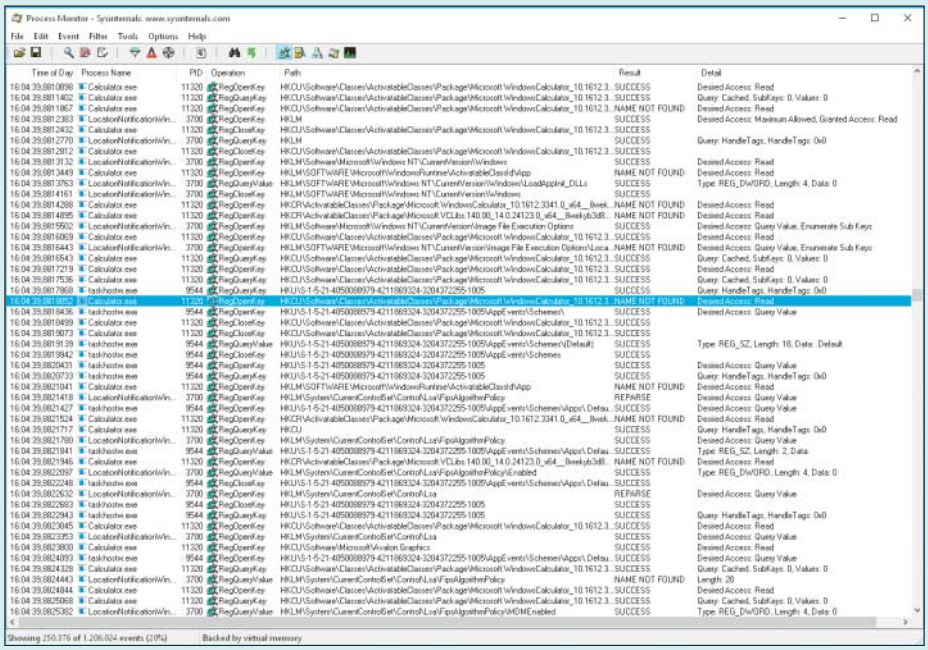
! Dazu exportieren Sie die Schlüssel beider Installationen jeweils zuerst in .reg-Dateien. Als Werkzeug zum Vergleichen taugen gängige diff-Programme für Textdateien wie die Freeware-Tools csdiff oder WinMerge (siehe c't-Link am Ende des Artikels).

Zuschauen

? Kann ich Windows dabei beobachten, auf welche Registry-Schlüssel es gerade zugreift?

! Ja, das geht, doch Obacht: Die Anzahl der Zugriffe ist normalerweise dermaßen hoch, dass Sie da sehr schnell den Überblick verlieren. Zudem brauchen Sie ein Programm dafür: den Process Monitor von Sysinternals (procmon.exe, siehe c't-Link). Der protokolliert sämtliche Zugriffe auf die Registry genauso wie auf Dateien und Ordner. Beim Durchsehen der Protokolle helfen sehr detailliert setzbare Filter. Tipps für erste Schritte damit finden Sie in [4].

Falls Ihnen bei der Durchsicht der Protokolle der Verdacht kommt, dass da Zugriffe fehlen, die eigentlich aufgezeichnet sein sollten, liegt es daran, dass Windows manche Schlüssel nur einmalig beim Hochfahren ausliest und dann nicht mehr. Das gilt zum Beispiel für die Einstellungen von Startmenü oder Explorer. Macht aber nichts: Im Process Monitor können Sie unter „Options“ den Eintrag „Enable Boot Logging“ auswählen. Darauf passiert scheinbar nichts, doch beim nächsten Booten von Windows protokolliert die Software nun alles mit, und zwar so lange, bis Sie das Programm wieder starten. Dann bietet es an, das Zugriffsprotokoll in eine Datei zu schreiben, die Sie später unter „File/Open“ öffnen und lesen können. *(hos@ct.de/axv@ct.de)*



Ein Protokoll der Registry-Zugriffe laufender Anwendungen wird sehr schnell so groß, dass man ohne sinnvolle Filterung in Daten ertrinkt.

Literatur

[1] Axel Vahldiek, Rettungsring Version 2, c't-WIMage erzeugt Sicherungskopien von Windows 8.1 und Windows 10, c't 5/16, S. 126

[2] Axel Vahldiek, c't-WIMage und Windows 10 Anniversary Update, c't 19/16, S. 162

[3] Axel Vahldiek, Unter dem Mikroskop, Tipps zum Umgang mit dem c't-Notfall-Windows, c't 26/16, S. 88

[4] Jan Schüßler, Totalüberwachung, Windows mit dem Sysinternals Process Monitor auf die Finger schauen, c't 20/16, S. 106

Registry-Tools: *ct.de/yscf*