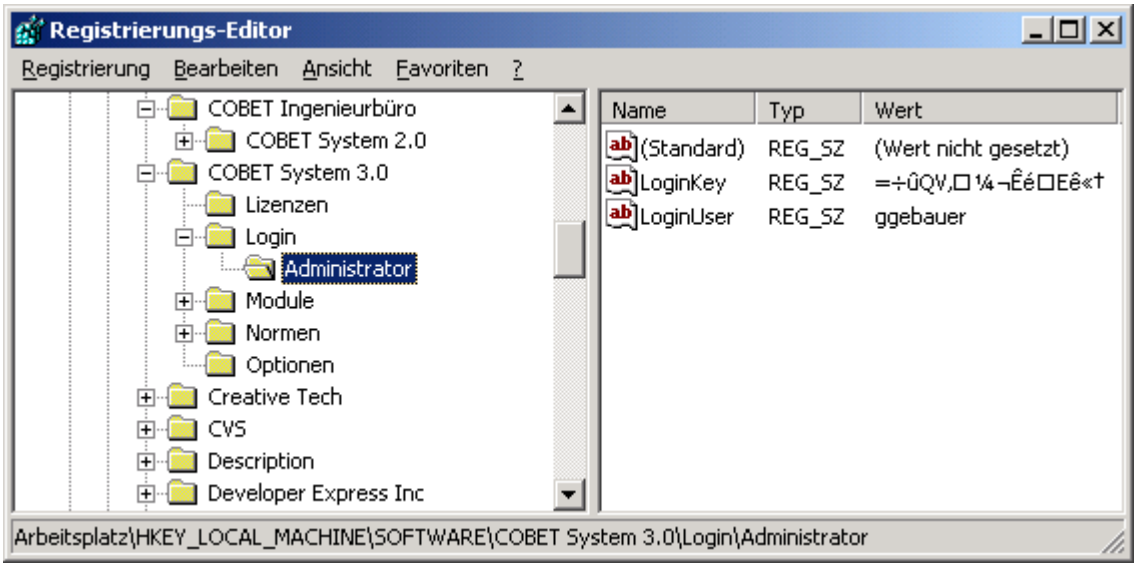
Administrative Verwaltung der automatischen COBET-Anmeldung

Grundprinzip der automatischen Anmeldung im COBET-System ist die Hinterlegung einer Verknüpfung zwischen einem Systembenutzer und dessen COBET-Anmeldung. Dabei werden sowohl der Anwender, als auch der Cobet-Benutzer sowie dessen Passwort (verschlüsselt) in der Registry hinterlegt. Die Verschlüsselung wird über die Kryptofunktionen des Dongle ausgeführt. Dadurch ist sichergestellt, dass keine Schlüssel zwischen verschiedenen COBET-Installationen ausgetauscht werden können.

Als Ablageort wird der Schlüssel "*HKEY_LOCAL_MACHINE\SOFTWARE\COBET System 3.0\Login*" verwendet. Der jeweilige Systembenutzer wird als Unterschlüssel angelegt, der als Werte "LoginUser" bzw. "LoginKey" die Angaben aus der COBET-Anmeldung enthält.



(ab Release 3.1.3.x fragt COBET optional auch den Schlüssel "*HKEY_CURRENT_USER\SOFTWARE\COBET System 3.0\Login*" ab)

Ablauf der Anmeldung

Beim Start des COBET-Programms wird zunächst der Name des angemeldeten System-Benutzers aus dem Betriebssystem abgefragt. Anhand dieser Angabe wird ein gleichnamiger Schlüssel unterhalb des Registry-Schlüssels " *HKEY_LOCAL_MACHINE \SOFTWARE\COBET System 3.0\Login*" gesucht. Wird dieser Schlüssel gefunden, werden die enthaltenen Daten (Nutzername und Passwort) ausgelesen und entschlüsselt. Anschließend erfolgt der normale Authentifizierungs- und Identifizierungsprozess, wie er im Programm auch nach der manuellen Eingabe von Namen und Passwort erfolgt.
Schlägt die Anmeldung fehl, verbleibt das Programm gestarteten Zustand, jedoch ohne angemeldeten Benutzer. Dies entspricht dem Zustand des Programms nach einem Start ohne automatische Anmeldung, d.h. der Anwender kann sich (über den Menüpunkt "Datei → Nutzer anmelden") mit dem normalen Anmeldebild-schirm anmelden.

Rahmenbedingungen

Die automatische Anmeldung bietet im Wesentlichen den Vorteil, ohne Eingabe eines Passwortes / Benutzers sofort nach dem Start mit dem COBET arbeiten zu können. Dieser Komfort ist allerdings mit gewissen Risiken verbunden. Bei Anwendungsvarianten, bei denen auf dem jeweiligen Rechner (Client bzw. Einzelplatzversion) nur ein Anwender vom Betriebssystem authentifiziert wird, sind keine Sicherheitsrisiken zu betrachten. Anders sieht es bei Systemen aus, bei denen mehrere Nutzer Zugriff auf den Rechner haben. Da die Registrierungs-daten den Namen des Anwenders enthalten, könnte sich ein Nutzer durch Umbenennen des Schlüssels Zugriff auf das COBET-System verschaffen.
(Beispiel: Benennt der Nutzer "USER" den Schlüssel "Administrator" im obigen Beispiel in "USER" um, kann er sich per automatischer Anmeldung unter dem COBET-Nutzer "ggebauer" anmelden und dessen Rechte übernehmen.)

In diesem Fall ist dafür zu sorgen, dass die Zugriffsrechte der Registry beschränkt werden. Im Wesentlichen kommen dafür folgende Verfahren in Frage.

a) Sperren des Schreibzugriffes für alle Nutzer auf den Schlüssel "Login" und dessen Unterschlüssel
b) Sperren des Schreibzugriffes der Nutzer auf alle Unterschlüssel von Login mit Ausnahme des eigenen Schlüssels.
c) Generelle Sperre für den Registry-Zugriff, d.h. der Zugriff auf entsprechende Bearbeitungsprogramme für die Registry wird gesperrt bzw. es wird nur das Starten definierter Programme ermöglicht (z.B. bei Terminal-Server-Lösungen)

Die Varianten a) und b) setzen voraus, dass die Aktivierung der automatischen Anmeldung bereits erfolgt ist, da sonst die entsprechenden Schlüssel fehlen und deren Anlegen entweder nicht mehr möglich (Variante a) oder ohne Schreibsperren für neue Einträge erfolgt (Variante b).
Zu Beachten ist, daß die Lesezugriffe natürlich nicht beschränkt werden dürfen, da sonst die Anmeldung nicht arbeiten kann.

Will der Administrator die automatische Einstellung vorkonfigurieren (z.B. für die Nutzung nach Variante a) gibt es folgende vereinfachte Möglichkeit. Als Voraussetzung sollte zunächst vom Administrator für einen der Anwender im COBET ein definiertes Passwort vergeben und dann die automatische Anmeldung mit diesem Passwort aktiviert werden. Das verschlüsselte Passwort steht nun im Werte "LoginKey" des Registry-Schlüssels des Anwenders (siehe oben).
Es werden nun alle anderen benötigten Paare aus Systembenutzer- und COBET-Benutzername als Schlüssel / Wertepaar erzeugt und das verschlüsselte Passwort des ursprünglichen Anwenders jeweils als Wert "LoginKey" in alle COBET-Anwenderschlüssel unter "Login" kopiert.
Wird im COBET nun für alle Anwender intern das identische Passwort vergeben, ist die automatische Anmeldung für alle Nutzer aktiviert.

Hinweis: Die Verschlüsselung des Passwortes arbeitet mit Binärdaten. Bei Kopiervorgängen in der Registry ist es möglich, dass bestimmte Zeichen deshalb nicht übertragbar sind und das Kopieren fehlschlägt. In diesem Fall kann man die ursprüngliche Aktivierung mit gleichem Passwort wiederholt ausführen. Da die Verschlüsselung mit stochastischen Funktionen arbeitet, entstehen bei mehrfacher Verwendung des gleichen Passwortes jeweils unterschiedliche Chiffrate.