HiCrypt 2.0 mit Tokenunterstützung

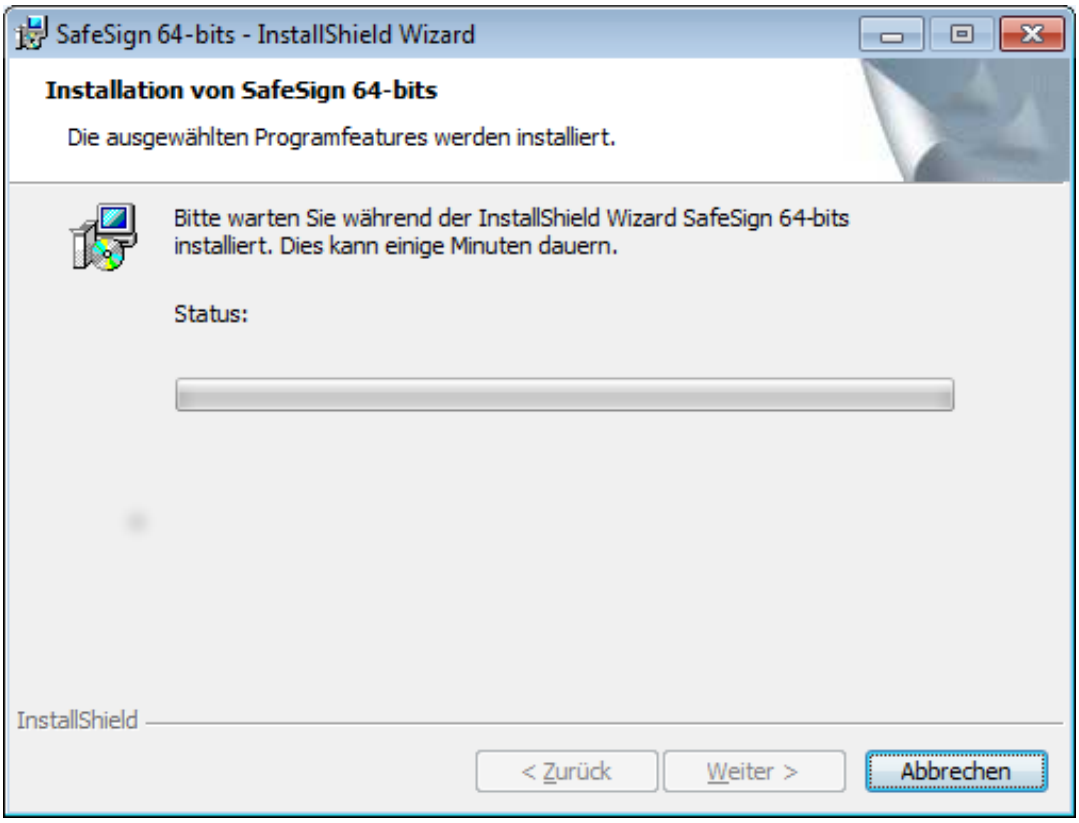
Um vertrauliche Daten im Unternehmen zu schützen und nur bestimmten, vom Datei-Besitzer ausgewählten Personen zugänglich zu machen, bietet digitronics mit HiCrypt 2.0 eine einfache Lösung. Ab Version 2.0 „mit Tokenunterstützung" kann die Sicherheit mit zwei-Faktor-Authentifizierung nochmals stark verbessert werden: Ein vom Datenbesitzer gesetztes Passwort alleine reicht nicht, auch der passende USB-Token muss den Besitzer ausweisen. So lässt sich auch ein Vier-Augen-Prinzip bewerkstelligen.

Zwei-Faktor-Authentifizierung

Hinter diesem Begriff verbirgt sich die Idee, dass neben einem statischen Passwort eine zweite Komponente den Nutzer identifizieren muss. So können Cyberkriminelle etwa Passwörter per Phishing oder Keylogger mitschnüffeln – ohne eine Chip- oder SMS-TAN wie beim Online-Banking oder einen USB-Token gilt der Nutzer als Fremd, die Daten werden nicht freigeschaltet.

Mit diesem Mechanismus lässt sich auch ein Vier-Augen-Prinzip durchsetzen, bei dem ein Anwender das Passwort besitzt und ein weiterer dann mit dem Dongle den Zugriff freischaltet.

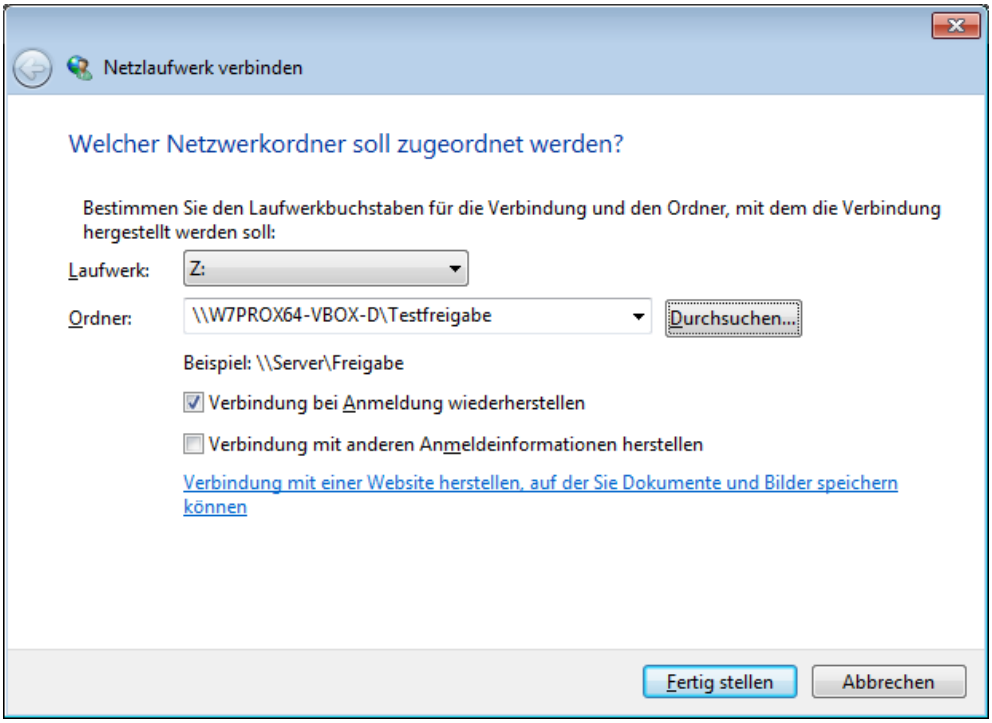
Für den USB-Token muss zunächst gegebenenfalls die benötigte Treibersoftware/Middleware installiert werden. Anschließend installiert man HiCrypt mit Unterstützung für Token.



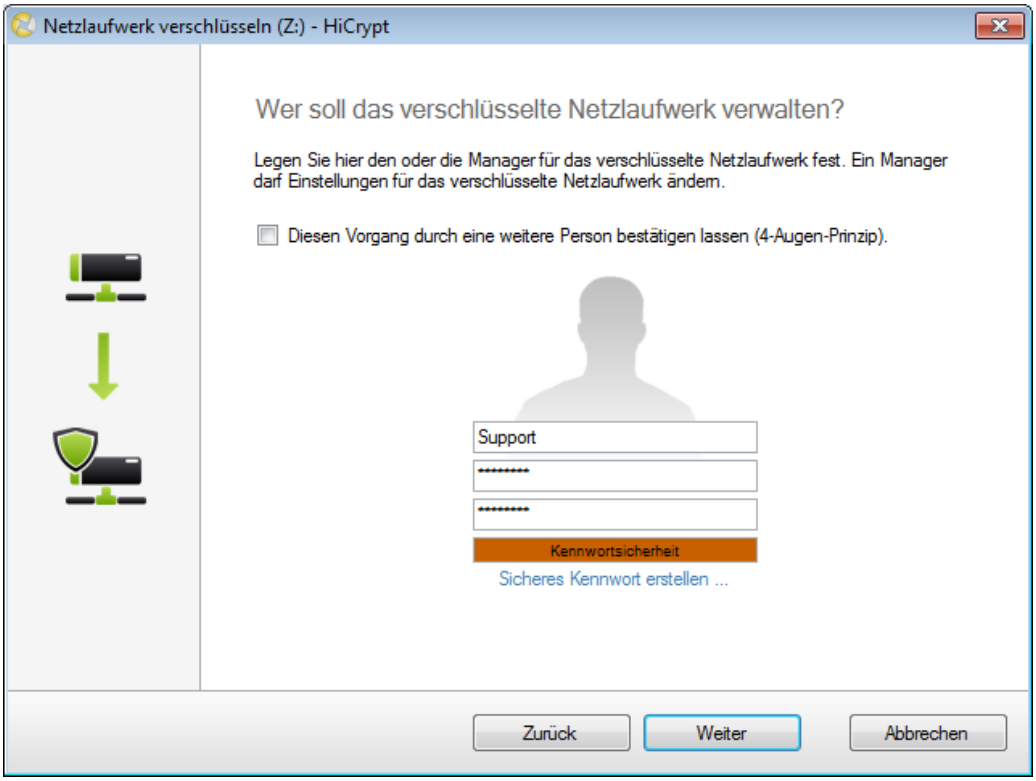
Installation der USB-Token-Software.

HiCrypt2.0-Installation mit Optionen zur Token-Verwendung.

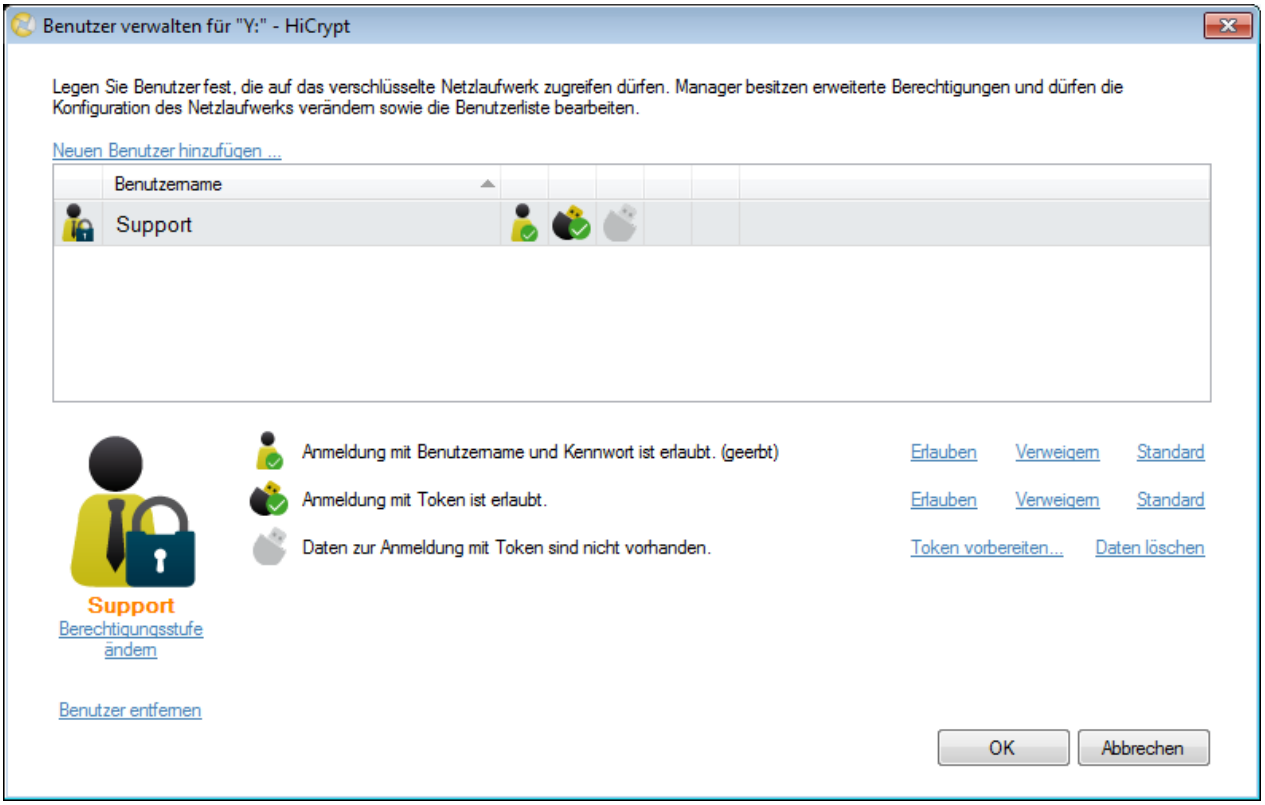
Laufwerke bindet man zunächst wie gewohnt ein.



Bei der Verschlüsselung des Laufwerks ist eine neue Option verfügbar – das Vier-Augen-Prinzip. Damit kontrollieren sich zwei Menschen gegenseitig und autorisieren die jeweils durchgeführte Aktion. Dies beginnt bereits beim Einrichten des Verwalters für ein verschlüsseltes Verzeichnis.

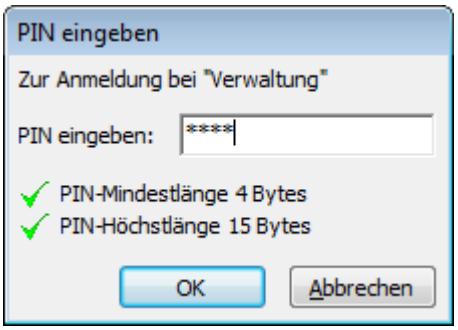


Bei einer verschlüsselten Freigabe ohne Vier-Augen-Prinzip kann man die Anmeldung mit Token unter der Benutzerverwaltung freischalten. Hier kann man nun auswählen, ob Benutzername und Passwort, der Token oder beides zum Freischalten erlaubt ist.



Durch Klick auf „Token vorbereiten" kann man den Token freischalten. Dazu muss man das Passwort eingeben.

Wenn man sich anschließend an einer verschlüsselten Freigabe anmelden möchte, kann man entweder Benutzername und Passwort verwenden oder via Anmeldung per Token arbeiten – je nachdem, was der Verwalter freigeschaltet hat. Für die Anmeldung mit Token steckt man diesen ein und muss die geheime PIN eingeben.



Aus Anmeldung mit festem Benutzernamen und Passwort wird dadurch also eine Anmeldung aus Passwort oder genauer einer PIN, die eine zusätzliche Hardware in Form des USB-Tokens benötigt. Eines der beiden Teile alleine reicht nicht, was die Sicherheit erhöht: Die Zwei-Faktor-Authentifizierung.

Der Token ist nur zum Freischalten nötig. Danach kann er abgezogen werden. Nach einem Neustart oder einer erneuten Anmeldung muss er natürlich wieder eingesteckt werden.

Weitere Informationen zu HiCrypt von Digitronic finden Sie unter:
https://www.jakobsoftware.de/digitronic/

Stand 7/2015