




SECURITY : CONSULTING : SHOP : INTEGRATION



**Signatory:** cryptoshop.com - Cryptas it-Security GmbH  
**Time:** UTC 2008-01-24, 11:28:41  
**ID:** 47 13 40 FA FD FE 05 9E 2B F1  
EA 61 4F 0D 50 01 A4 72 AA EA  
**Reason:** digital source document confirmation  
**Location:** Austria  
**Remarks:** This signature was done with xyzmo Server 3.0  
**Attachments:** none

*xyzmo* seal [www.xyzmo.com](http://www.xyzmo.com)



Click to Verify *xyzmo* 



# Winmagic SecureDoc Enterprise Server 4.3.1

## Verwaltung

**CRYPTAS it-Security GmbH**

Modecenterstrasse 22/B2  
A-1030 Wien

[www.cryptoshop.com](http://www.cryptoshop.com)  
[www.cryptas.com](http://www.cryptas.com)

## Allgemeines

SecureDoc Enterprise Server bietet eine Vielzahl von Einstellungsmöglichkeiten und lässt sich an fast jede denkbare Umgebung und fast jeden Bedarf anpassen. Das beginnt mit einfachen Firmen ohne Gefährdung und geht bis zu hochkomplexen Organisationen mit ausgefallenen Ansprüchen und sehr sensiblen Daten. Jede dieser denkbaren Konfigurationen hat selbstverständlich auch andere Ansprüche an die Verwaltung. So sind beispielsweise Clienteneinstellungen innerhalb eines Standortes anders hand zu haben als die Einstellungen von verstreuten Computern, die teilweise nicht einmal über eine Netzwerkverbindung verfügen.

Wir wollen hier nun einige Beispiele von einfachen und oft vorkommenden Verwaltungsaufgaben in einer einfachen Struktur kennenlernen.

## Hinzufügen von Benutzern zu Geräten

In manchen Unternehmen ist es üblich, dass mehrere Benutzer an einem Computer arbeiten oder dass Benutzer sich einfach an einem gerade freien Gerät anmelden (dazu gibt's ja eigentlich Active Directory Domänen und servergespeicherte Profile).

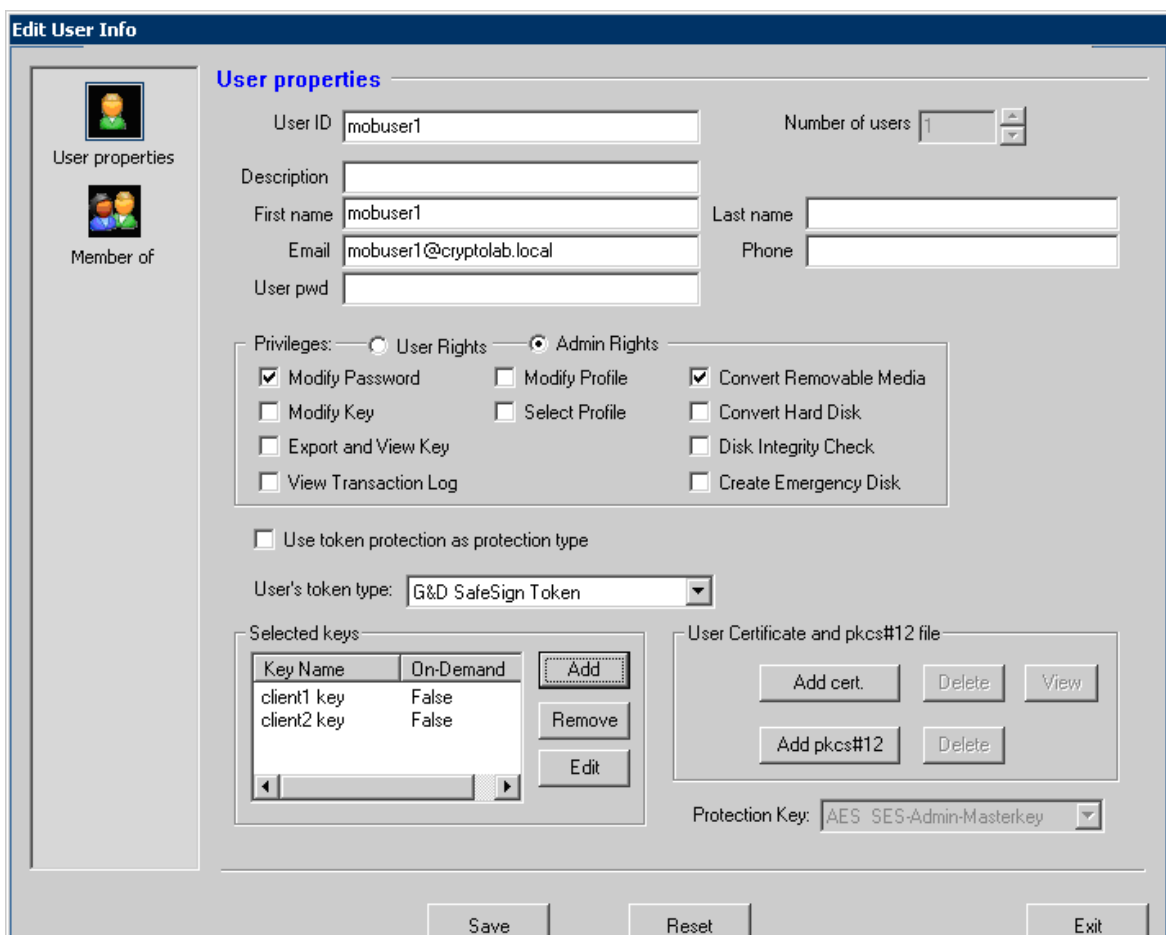
Um diese Funktionalität zu ermöglichen und dennoch die Informationen auf den Festplatten gegen den Zugriff Unbefugter zu schützen (die Festplatten sind ja verschlüsselt und daher ist ein Logon notwendig, bevor das Betriebssystem startet) müssen die jeweiligen Benutzer auf den „Keyfiles“ der einzelnen Computer berechtigt werden. Sie brauchen Zugriff auf den Schlüssel, um den Computer starten zu können.

Wir öffnen also die Management Konsole und authentisieren uns gegen das Keyfile mit der notwendigen Berechtigung, den Container (Folder) zu verwalten.

Nun sind 2 Schritte notwendig:

- 1.) wir fügen dem Benutzerkonto den/die Schlüssel der Computer hinzu
- 2.) wir fügen den/die Benutzer zu den Computer als Berechtigte hinzu

Wir klicken rechts auf den Benutzer und wählen „**modify user**“ und fügen mit „**add**“ alle notwendigen Computerschlüssel dem Schlüsselbund des Benutzers hinzu:

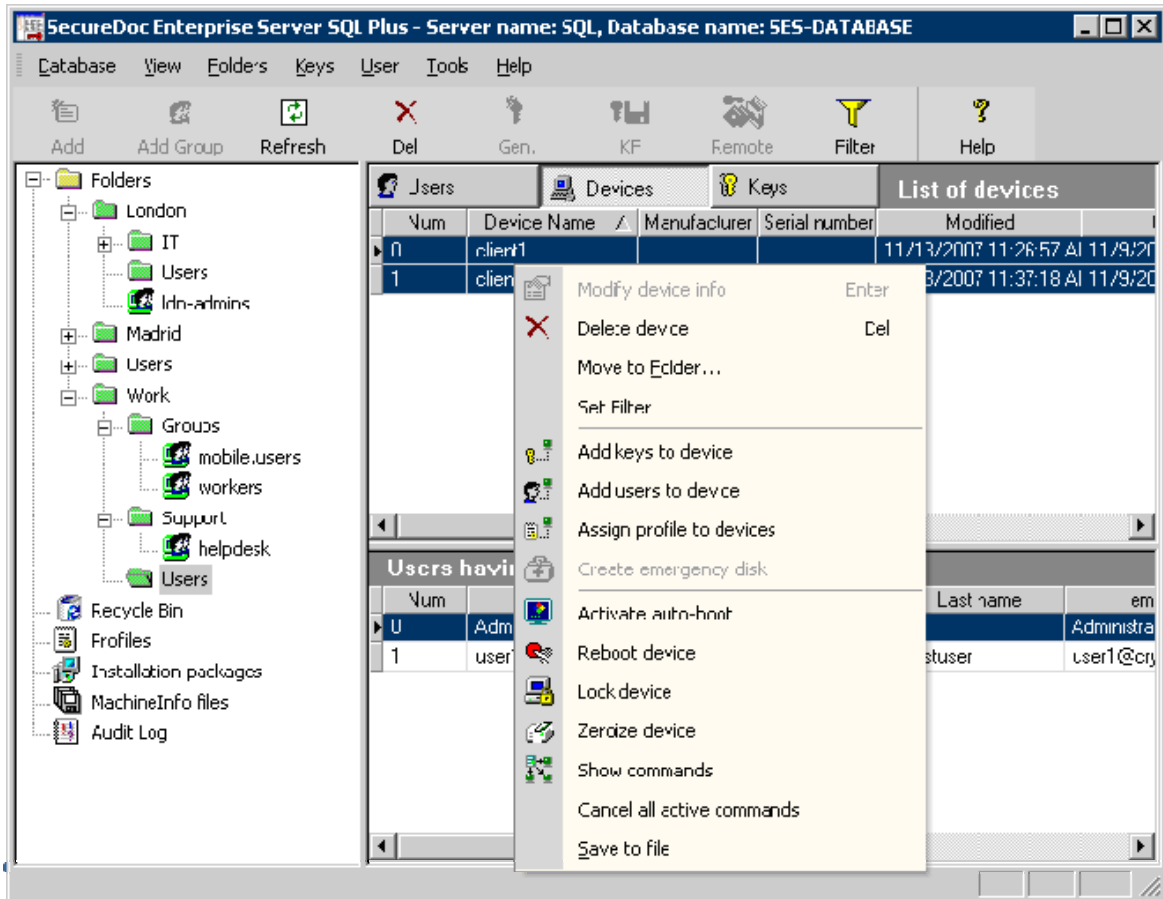


Key Name	On-Demand
client1 key	False
client2 key	False

Hier können wir uns nun auch aussuchen, ob der „Schlüsselbund“ des Benutzers durch ein Passwort („**User pwd**“) oder durch eine Smartcard oder ein Token geschützt werden soll. In diesem Falle markieren wir einfach „**Use token protection...**“ und wählen das von unserem Benutzer verwendete Token aus.

Mit „Save“ verlassen wir diesen Benutzer

Nun wählen wir einen oder mehrere Computer aus und klicken mit der rechten Maustaste auf sie....



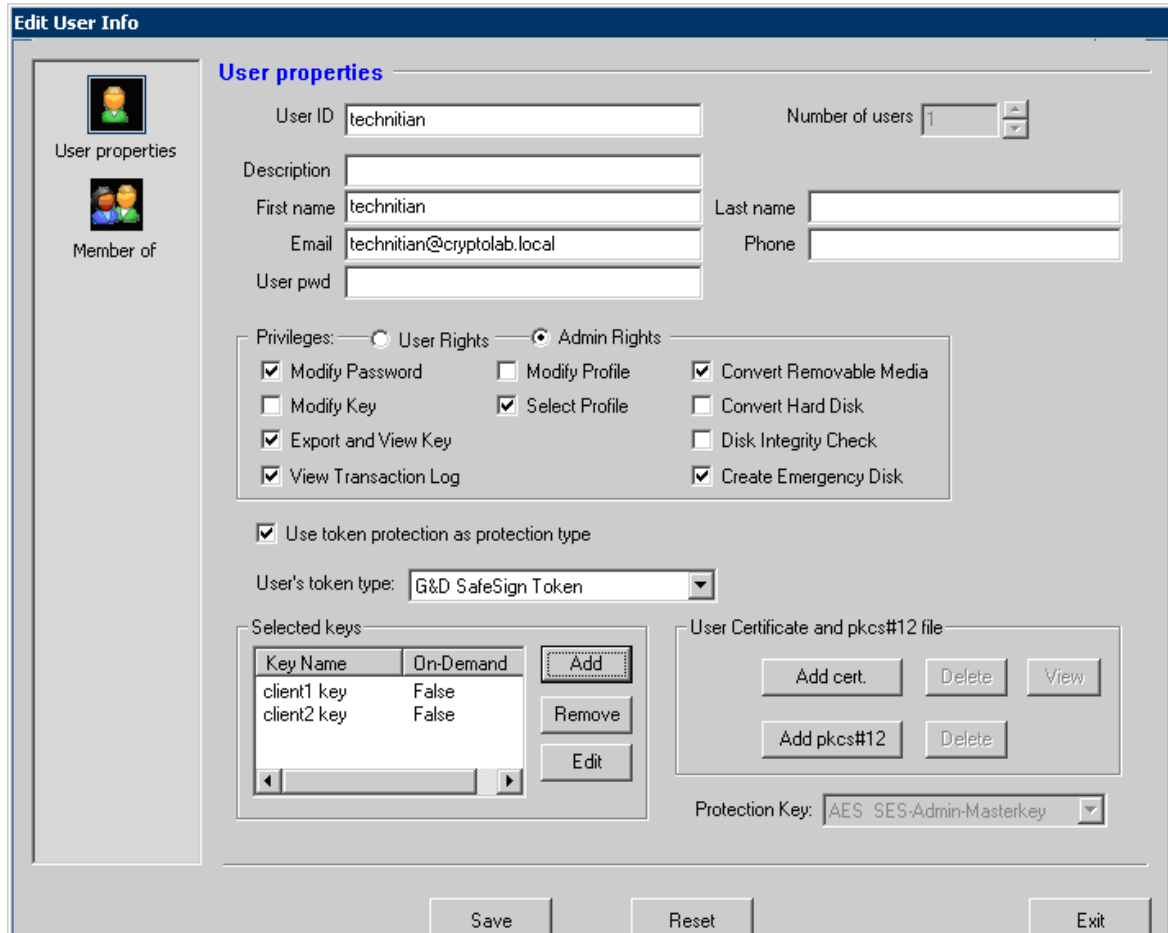
## Hier fehlen 2 Screenshots und die dazugehörige Beschreibung

Wenn Sie an der vollständigen Version des Dokumentes interessiert sind, kontaktieren Sie uns bitte unter [sales@cryptas.com](mailto:sales@cryptas.com).

## Ändern von Benutzerrechten

Um etwa einen „Poweruser“ zu erstellen oder einem Helpdesk Mitarbeiter die Möglichkeit zur technischen Hilfeleistung zu geben, erweitern wir die Rechte eines oder mehrerer Benutzer

-> Rechts click auf den Benutzer



Key Name	On-Demand
client1 key	False
client2 key	False

„save“ und fertig. Die neuen Einstellungen werden wieder automatisch an die zugeordneten Computer übertragen.

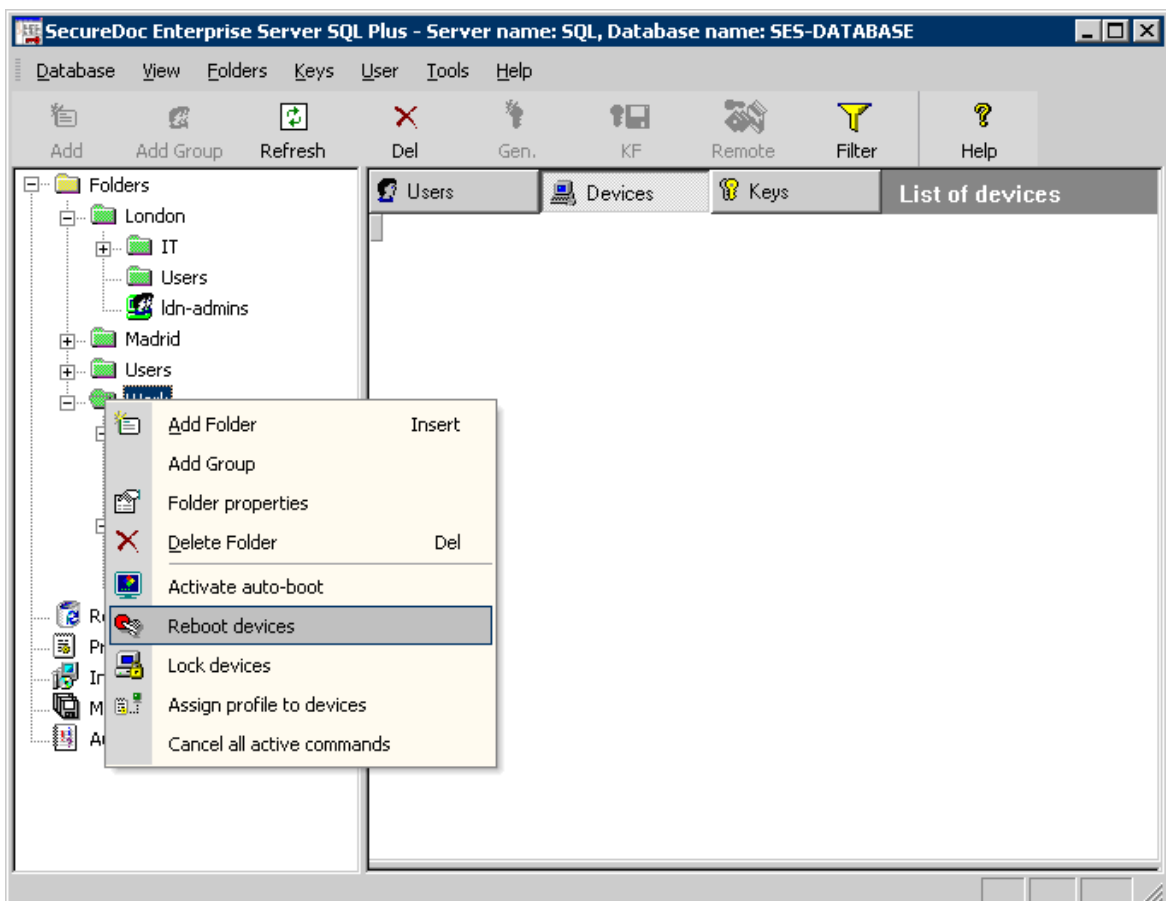
## Ausführen von „Remote Commands“

SES bietet die Möglichkeit, eine kleine Zahl an Kommandos auf remote Computern auszuführen. Diese Kommandos beziehen sich ausschließlich auf die Festplattenverschlüsselung und die Auswirkungen, die das Preboot Logon auf die Softwareverwaltung eines Unternehmens hat.

## Hier fehlt 1 Screenshot und die dazugehörige Beschreibung

Wenn Sie an der vollständigen Version des Dokumentes interessiert sind, kontaktieren Sie uns bitte unter [sales@cryptas.com](mailto:sales@cryptas.com).

Ein Teil dieser „remote commands“ ist auch für Container verfügbar und betrifft alle Client Geräte, die innerhalb dieses Containers angelegt wurden.



## Konvertierung von Passwort Schutz zu Smartcards oder Smart Token

Der Schutz der Daten auf den Computern und auf den verschlüsselten Medien steht und fällt mit dem Schutz des „Keyfiles“. Wer Zugriff auf den Schlüsselbund hat, hat auch unbegrenzten Zugriff auf alle für diesen Benutzer oder auf diesem Gerät verschlüsselten Informationen.

Zwar ist das Keyfile (ähnlich wie eine Bank Karte) mit einem Zähler ausgestattet, der das Keyfile nach einer einstellbaren Anzahl von Fehlversuchen sperrt, sodass ein beliebiges Raten am Gerät einen Angreifer nicht zum Ziel führt, dennoch bleibt das Passwort ein schwacher Schutz. Jeder, der das Passwort kennt, hat Zugriff und Passworte können auf vielerlei Art an Unbefugte geraten. So kann es etwa sein, dass ein Benutzer ein sehr schlechtes Passwort wählt (mangelnde Richtlinien), welches dann leicht zu erraten ist (z.B. Firmenname) oder es sich gerade wegen der bestehenden Richtlinien einfach irgendwo aufschreibt (Unterseite der Tastatur, Unterseite des Notebooks). Des weiteren kann es sein, dass der Benutzer das Passwort jemandem verrät und dieses dann als „gemeinsames Gut“ überall hin weiter erzählt wird.

Hat man nun den Bedarf nach mehr Schutz, so muss man den Benutzer dazu anhalten, eine Authentisierung mit mehr als einem Faktor zu benutzen -> Smartcard oder Smart Token. Hier hat er einen Pin UND einen Gegenstand, der mitzuführen ist. Den Pin könnte der Benutzer wohl noch aufschreiben oder weitererzählen, aber einfach nur die Pin zu wissen, nutzt einem Angreifer nichts, er würde auch noch das Token oder die Smartcard benötigen, die der Benutzer (hoffentlich) bei sich trägt.

Will man dann ganz sicher sein, kann man das Token oder die Smartcard an den Benutzer binden, indem man ein biometrisches Merkmal anstelle des Pin verwendet (Fingerabdruck). In diesem Falle kann der Benutzer seine Karte oder sein Token nicht mehr verborgen.

Wir implementieren in unserer Beispielinstantiation nun mittlere Sicherheit, indem wir eine Smartcard verwenden, die durch einen Pin geschützt ist.

Dazu konfigurieren wir nun einen vorhandenen Benutzer dazu, ausschließlich mittels seiner Smartcard auf das Keyfile zuzugreifen. Wir öffnen wieder die Management Konsole und authentisieren uns gegen das Keyfile mit der Admin Berechtigung. Dann wählen wir einen Benutzer aus (rechts click) und wählen „modify user“

## Hier fehlt 1 Screenshot und die dazugehörige Beschreibung

Wenn Sie an der vollständigen Version des Dokumentes interessiert sind, kontaktieren Sie uns bitte unter [sales@cryptas.com](mailto:sales@cryptas.com).

Nun müssen wir nur mehr warten, bis das geänderte Keyfile des Benutzers auf den/die zugeordneten Computer automatisch übertragen wird. (Tip: wir können den die Zuordnung des Benutzers zum Computer entfernen und wiederherstellen, um eine sofortige Übertragung zu erzwingen)



Der Benutzer „Test“ startet nun seinen Computer, indem er seine Smartcard einlegt und seinen Pin eingibt.

Es ist ihm nicht mehr möglich, den Computer ohne seine Smartcard zu starten:



Um einen vollständigen Schutz der Informationen auf einem Gerät zu erreichen, müssen selbstverständlich alle zugeordneten Benutzer von Passwort auf Smartcard umgestellt werden.

#### Stärkste Sicherheit:

Wir können nun den Pin, der zum Zugriff auf Smartcard oder das Token notwendig ist, durch ein biometrisches Merkmal, wie etwa einen Fingerabdruck ersetzen. Dazu müssen folgende Voraussetzungen erfüllt sein:

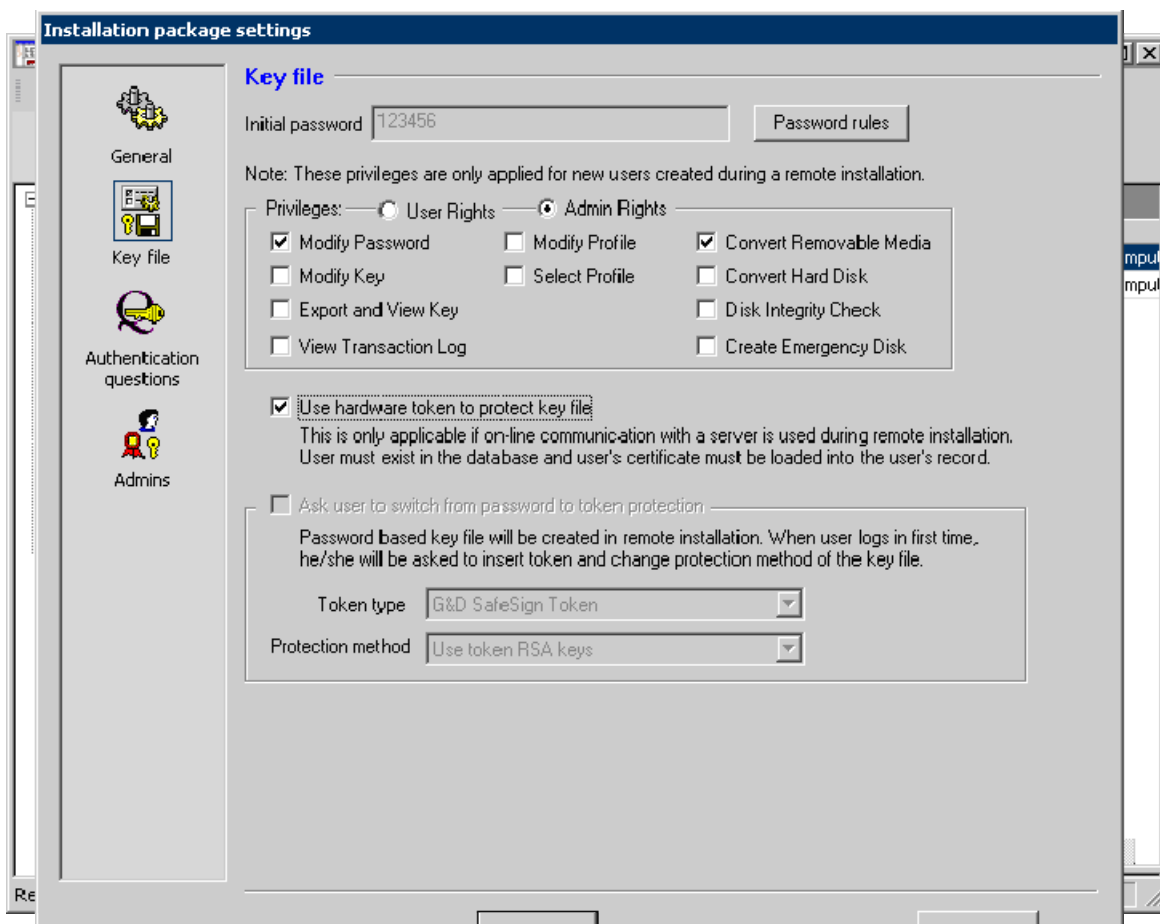
- unsere Client Geräte müssen mit einem passenden Lesegerät für dieses Merkmal ausgerüstet sein (Beispiel: **Precise 200 MC** von Precise Biometrics)
- Unsere Smartcards oder Smart Token müssen die Fähigkeit zur Biometrischen Authentisierung haben. Die Biometrische Authentisierung muss aktiviert und ausgerollt sein.
- Unsere Smartcards oder Smart Token müssen von Winmagic SecureDoc unterstützt werden.

Eine überprüfte und funktionierende Karte, die beiden Anforderungen genügt wäre **Safenet Model 330 G**.

## Rollout mit starker Authentisierung (Smartcards oder Smart Token) anstelle von Passwörtern

Wir können gleich im Rollout der SecureDoc Client Software auf starker Authentisierung für alle Benutzer bestehen.

Dazu müssen wir ein Installationspaket erstellen, indem dieses gefordert wird.



In den Keyfile Optionen des Installationspaketes haben wir nun 2 Möglichkeiten:

- Eine einfache Konfiguration für eine verwaltete Umgebung. Die Computer sind während der Installation des Clients online, wir verwenden Benutzer die bereits in der SES Datenbank angelegt sind (aus einem Verzeichnis importiert oder manuell erstellt) und die Benutzer müssen bereits mit einer Smartcard oder Token Anmeldung ausgestattet sein.
- Eine Konfiguration, die es uns erlaubt, auch Geräte, die während der Installation nicht online sind, oder sogar nie online gehen mit starker Authentisierung zu schützen. Diese verwenden wir auch, wenn wir die Benutzer während der Installation erstellen lassen bzw., wenn wir von typischen Smartcards abweichende Token Lösungen verwenden wollen. Hier können wir das dort verwendete Token und den Schutz auswählen. Allerdings ist hier eine Benutzerinteraktion nach der Installation des Clients notwendig (durchaus anspruchsvoll und sollte von einem Helpdesk Mitarbeiter angeleitet werden)

Wir wählen in unserer Beispielinstallation eine einfache Konfiguration und erstellen die Paketdateien. Mit diesen Paketdateien wird dann auf allen betroffenen Computern SecureDoc installiert.

Wichtig: Alle nachträglich hinzugefügten Benutzer müssen ebenfalls zur Authentisierung mittels Smartcard konfiguriert sein (siehe oben). Sollte das nicht so sein, kann der Schutz des Computers unterlaufen werden und die Nutzung des Computers ist ohne starke Authentisierung möglich. (Gefahr: Benutzername + Passwort auf einem Zettel an der Rückseite der Tastatur oder so etwas in der Art).

CRYPTAS it-Security GmbH  
Modecenterstrasse 22/B2  
A-1030 Wien, Austria  
T +43 (1) 798 96 96 – 0  
F +43 (1) 798 96 96 – 99  
info@cryptas.com

[www.cryptoshop.com](http://www.cryptoshop.com)  
[www.cryptas.com](http://www.cryptas.com)