



SECURITY : CONSULTING : SHOP : INTEGRATION



Signatory: cryptoshop.com - Cryptas it-Security GmbH
Time: UTC 2008-01-24, 11:26:09
ID: EF 43 2F 5F 84 BF EC 23 09 BA
BA 5A 73 5C 54 49 A7 A2 FC 96
Reason: digital source document confirmation
Location: Austria
Remarks: This signature was done with xyzmo Server 3.0
Attachments: none

xyzmo seal www.xyzmo.com



Click to Verify *xyzmo* 



Winmagic SecureDoc Enterprise Server 4.3.1

Betrifft Benutzer

CRYPTAS it-Security GmbH

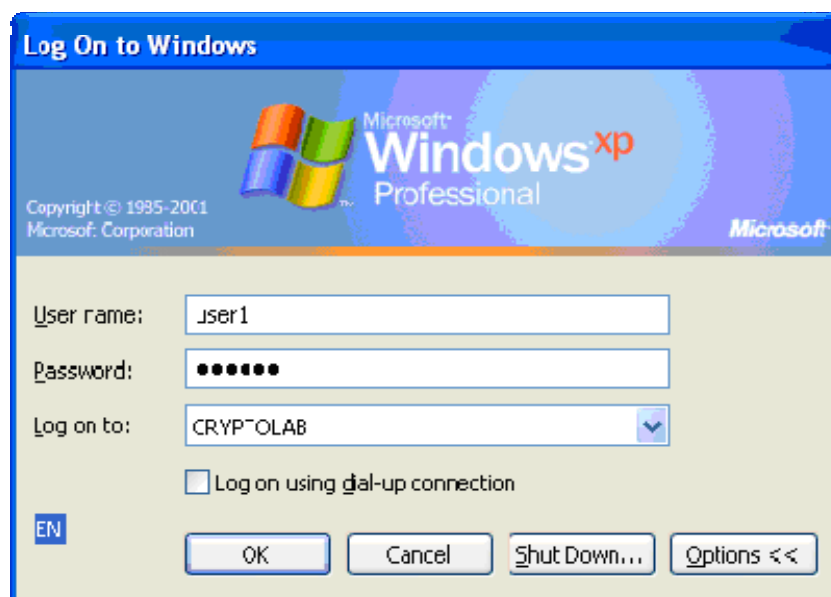
Modecenterstrasse 22/B2
A-1030 Wien

www.cryptoshop.com
www.cryptas.com

Installation der Clientsoftware

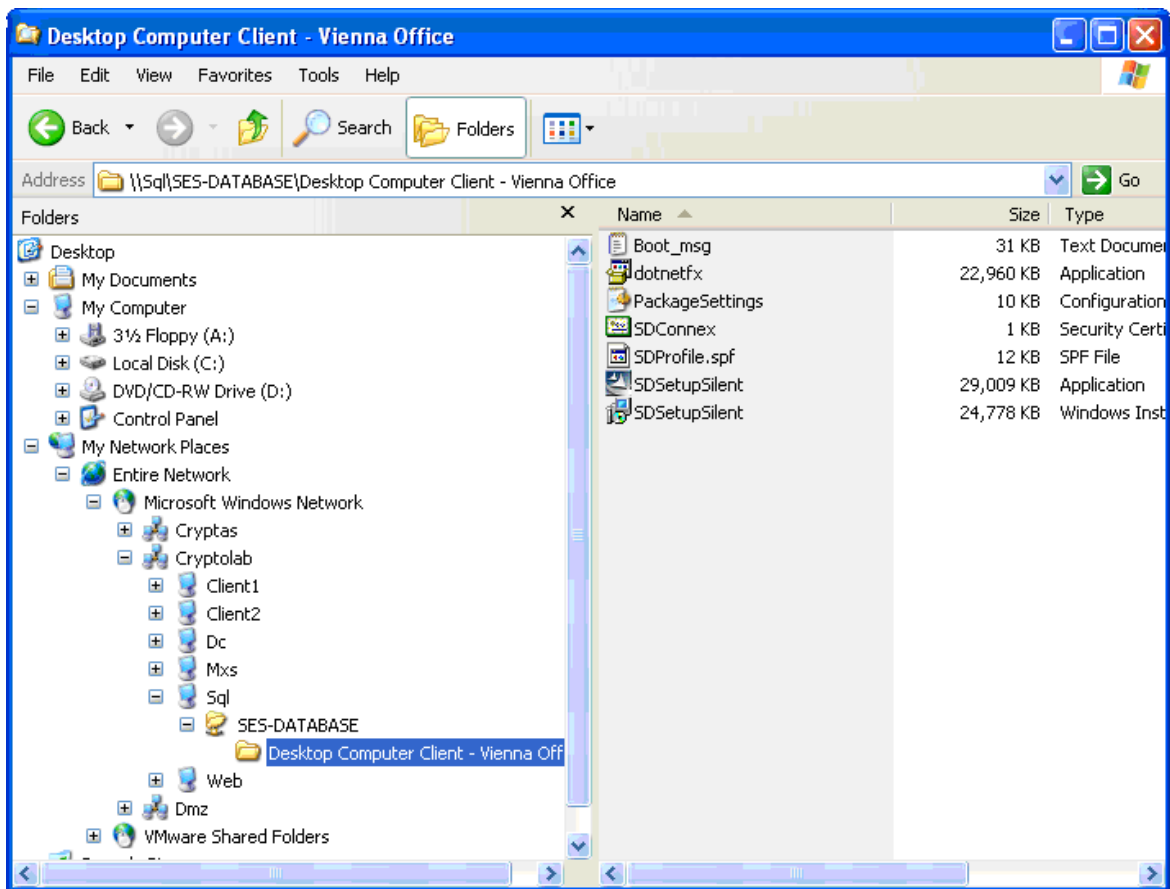
Um den Vorgang der Installation kennenzulernen, führen wir eine manuelle Beispielinstallation an einem Client Computer durch. Wir melden uns an einem Client Computer, der einer der vorgesehenen Computerklassen entspricht (anhand dieser Einteilung haben wir im SES angepasste Profile und Installationspakete erstellt), als Benutzer an.

In unserem Falle verwenden wir einen typischen „Desktop Computer“ mit Windows XP SP2 und MS Office ohne zusätzliche Anpassungen, sozusagen „out of the box“. Er ist Mitglied der Active Directory Domain „Cryptolab“ und hat eine direkte TCP/IP Verbindungen zu den Servern dieser Umgebung.



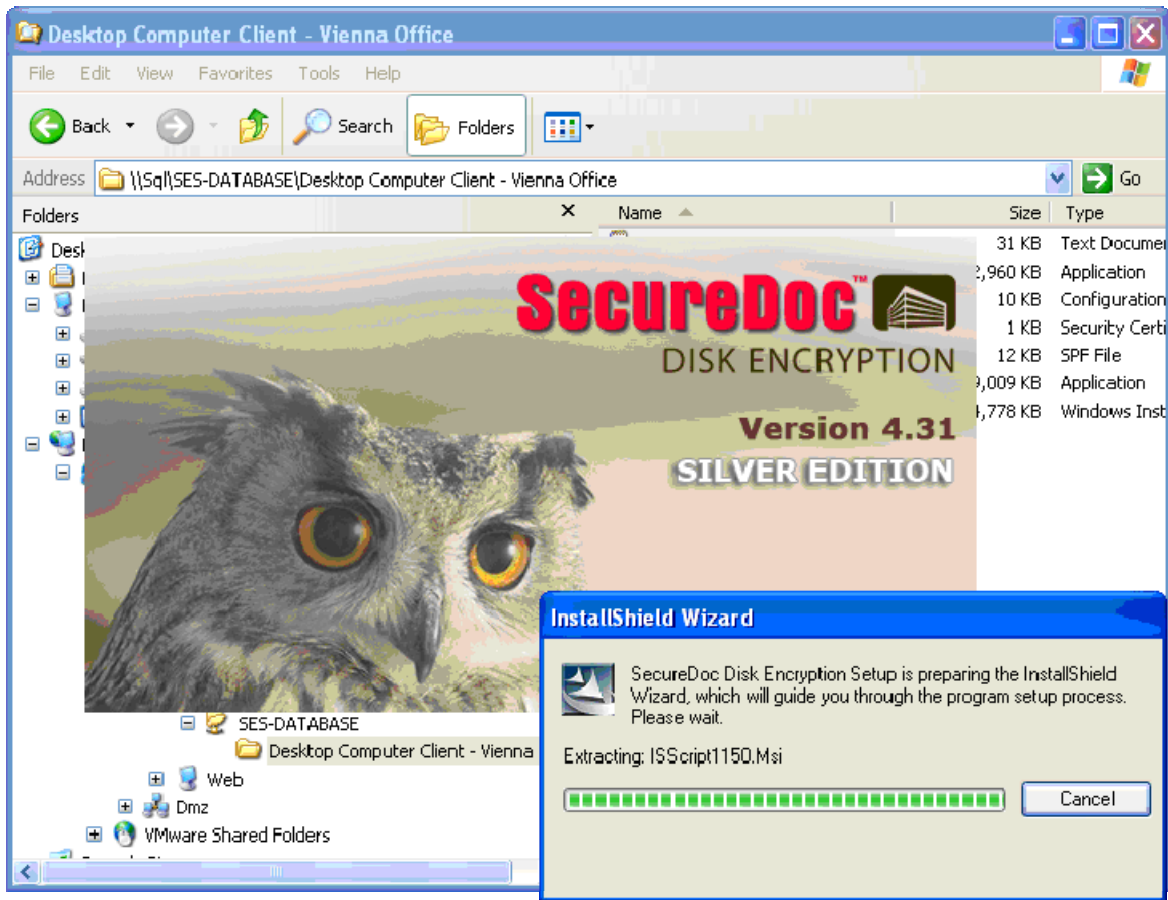
Wir erinnern uns: SecureDoc benötigt zur Installation am Client Computer lokale administrative Rechte und in den von uns hier verwendeten Paketeinstellungen muss es im Kontext des Benutzers installiert werden (wir verwenden den Namen des angemeldeten Benutzers anstelle von Computernamen oder frei wählbaren Namen). Also wurden dem Benutzerkonto (Domain User) vom zuständigen Helpdesk für die Installation lokale administrative Rechte erteilt, die nach der Installation wieder rückgesetzt werden können.

Wir öffnen nun die Netzwerkfreigabe, auf der das für uns vorgesehene Installationspaket angeboten wird.



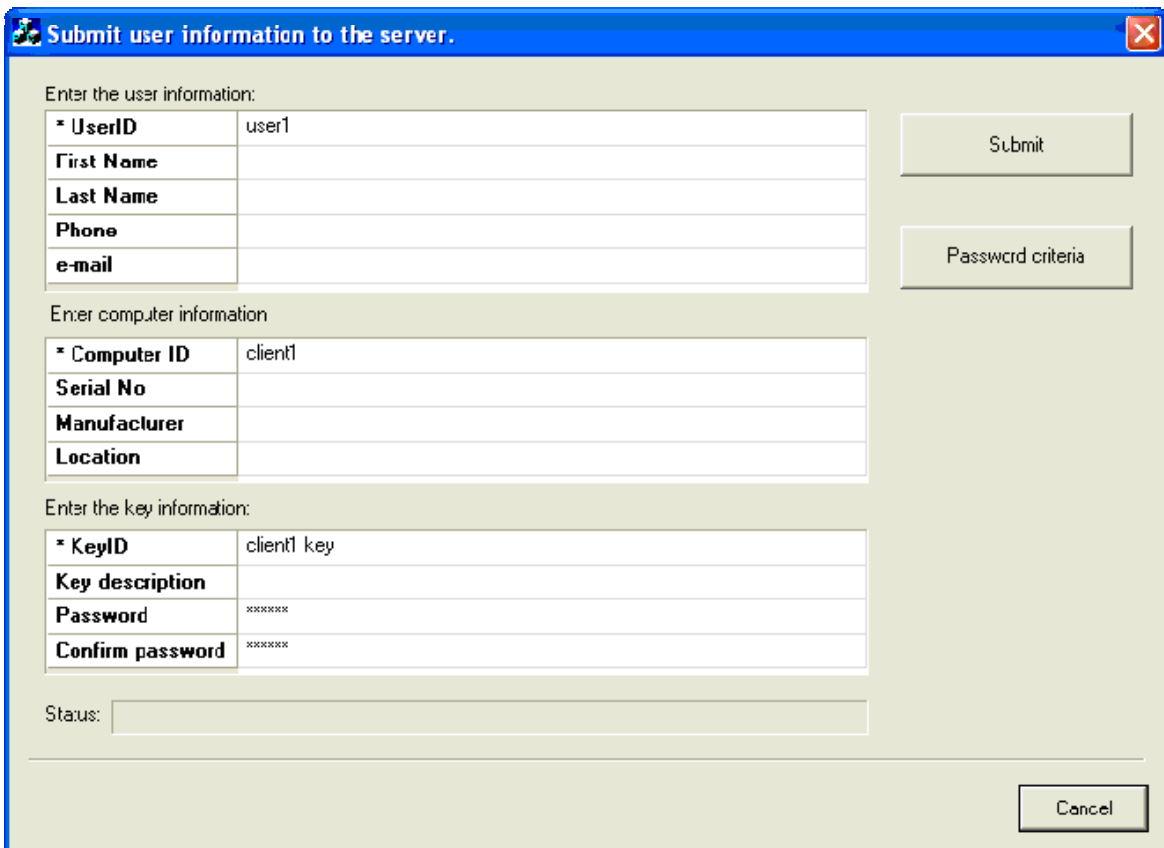
Auf dem Computer muss Microsoft .Net Framework 2.0 installiert sein. Wenn das nicht der Fall ist, kann es mit der Setupdatei dotnetfx.exe nachinstalliert werden.

Wir führen nun die Installationsdatei SDSetupSilent.exe aus



Das war es auch schon.....

..... und einen Herzschlag später erscheint (wenn wir es im Paket so eingestellt haben) der Dialog zum Bestätigen der Benutzer und Computerdaten. Wenn wir zum befüllen der Datenbank mit dem AD synchronisieren, ist hier keine Interaktion notwendig und der Dialog müsste auch nicht angezeigt werden. Wenn wir aber beschlossen haben, die Benutzer und Computerinformationen während der Installation einpflegen zu lassen, muss dieses Formular vom Benutzer ausgefüllt werden.



Submit user information to the server.

Enter the user information:

| | |
|------------|-------|
| * UserID | user1 |
| First Name | |
| Last Name | |
| Phone | |
| e-mail | |

Enter computer information:

| | |
|---------------|---------|
| * Computer ID | client1 |
| Serial No | |
| Manufacturer | |
| Location | |

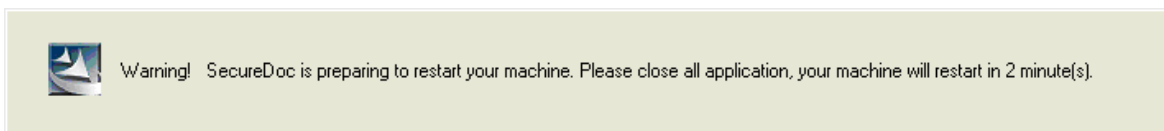
Enter the key information:

| | |
|------------------|-------------|
| * KeyID | client1 key |
| Key description | |
| Password | ***** |
| Confirm password | ***** |

Status:

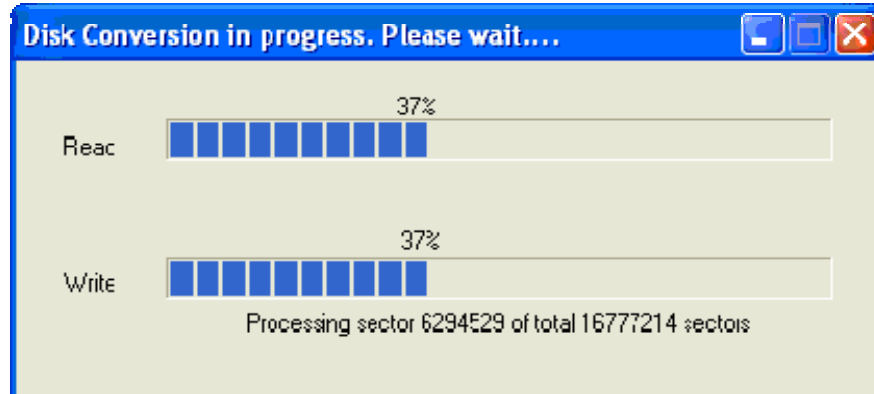
Buttons: Submit, Password criteria, Cancel

-> „Submit“



Wenn es im Paket so eingestellt wurde, wird der Computer sofort neu gestartet und der Vorgang gleich fortgesetzt. Sonst wartet Setup mit dem Neustart auf das nächste Herunterfahren durch den Benutzer oder das Kommando von der Verteilungssoftware (SMS, Tivoli... der übliche, geplante Mitternachtsstart:-)

Nach dem Neustart und dem Anmelden wird dann der Computer von Securedoc in den im Profil angegebenen Zustand versetzt. In unserem Fall haben wir im Profil beschlossen, die Festplatte des Computers vollständig zu verschlüsseln und ein PreBoot Logon zu installieren.

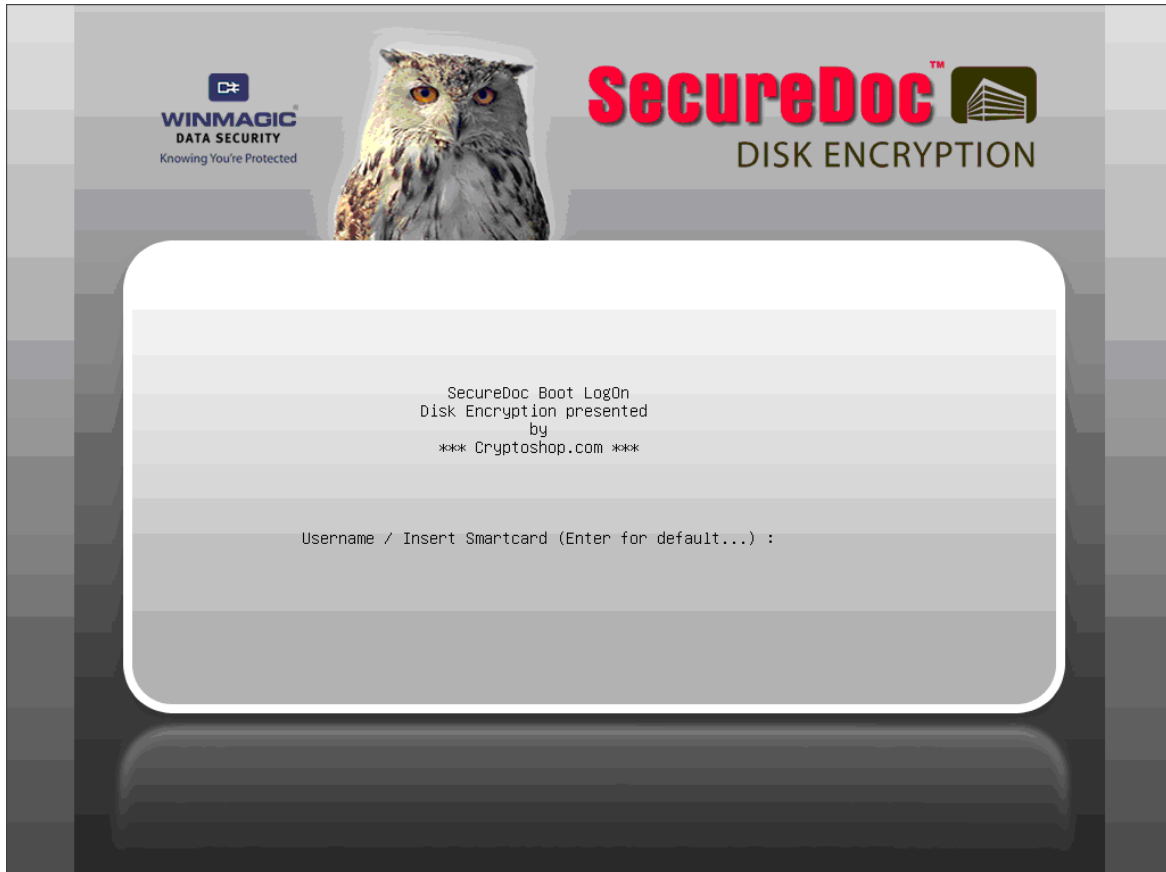


Dieses Informationsfenster kann wahlweise angezeigt werden oder auch nicht. Wenn nicht, läuft die Konvertierung vollständig unsichtbar im Hintergrund ab. Anschließend muss der Computer noch einmal neu gestartet werden. Das geschieht wieder, entsprechend der Einstellungen des Paketes, automatisch gleich, durch den Benutzer oder durch die Verteilungssoftware.

Der Daten auf dem Computer sind nun geschützt

Erste Schritte / Logon / Fragen und Antworten:

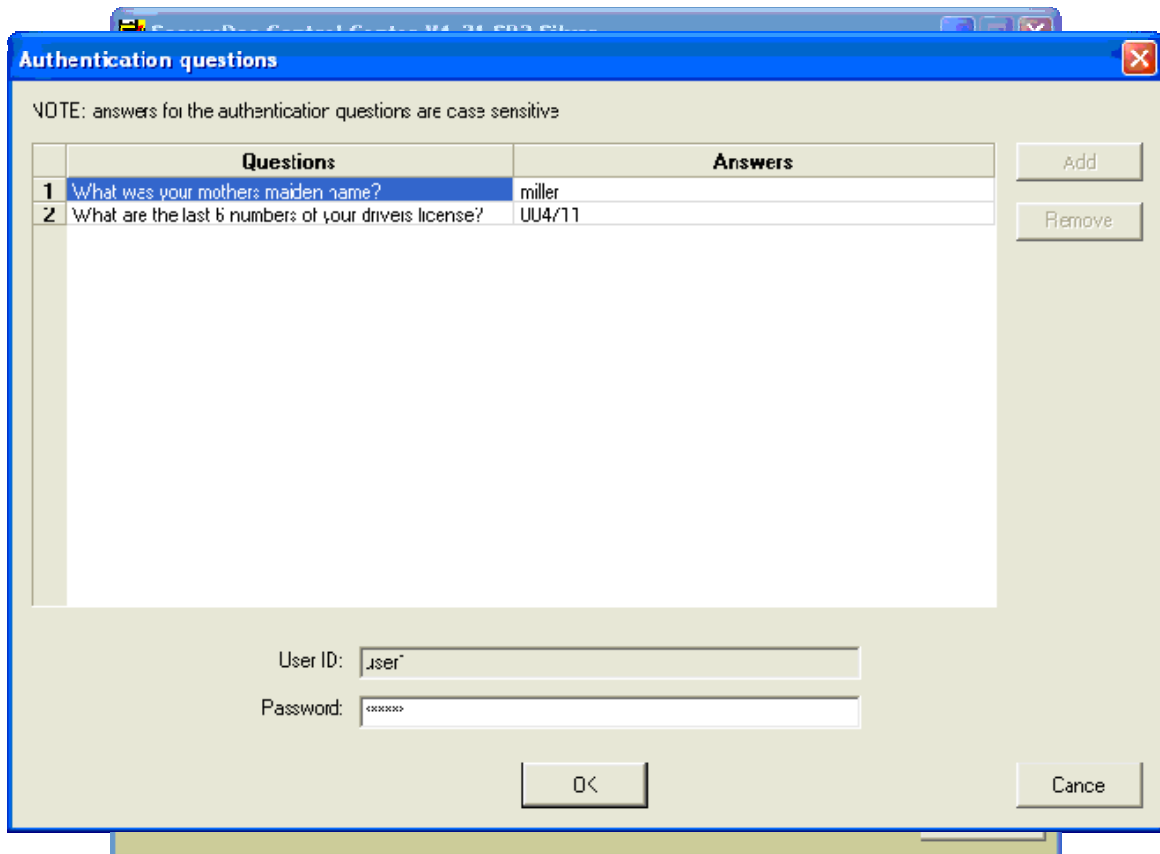
Wenn ein Benutzer einen geschützten Computer startet, so muss er zuerst ein Startpasswort eingeben.



Das ist nicht vergleichbar mit dem Startpasswort des BIOS, da das BIOS nur den Start selbst verhindern oder zulassen kann. Wenn ein Angreifer die Festplatte ausbaut und an einen anderen Computer anschließt, sind ihm sowohl die Daten, als auch alle gespeicherten Profile (und damit „private Keys“ und gespeicherte Passworte) zugänglich. Das Startpasswort von SecureDoc hingegen ermöglicht den Zugriff auf den „Schlüsselbund“ des Computers, das „Keyfile“ und ermöglicht es so, das ebenfalls verschlüsselte Betriebssystem zu starten bzw. die verschlüsselte Festplatte zu lesen. Ohne diesen Zugang, können die Informationen auf der Festplatte auch nicht von sogenannten „Datenrettern“ mit ihren fortschrittlichen technischen Möglichkeiten ausgewertet werden.

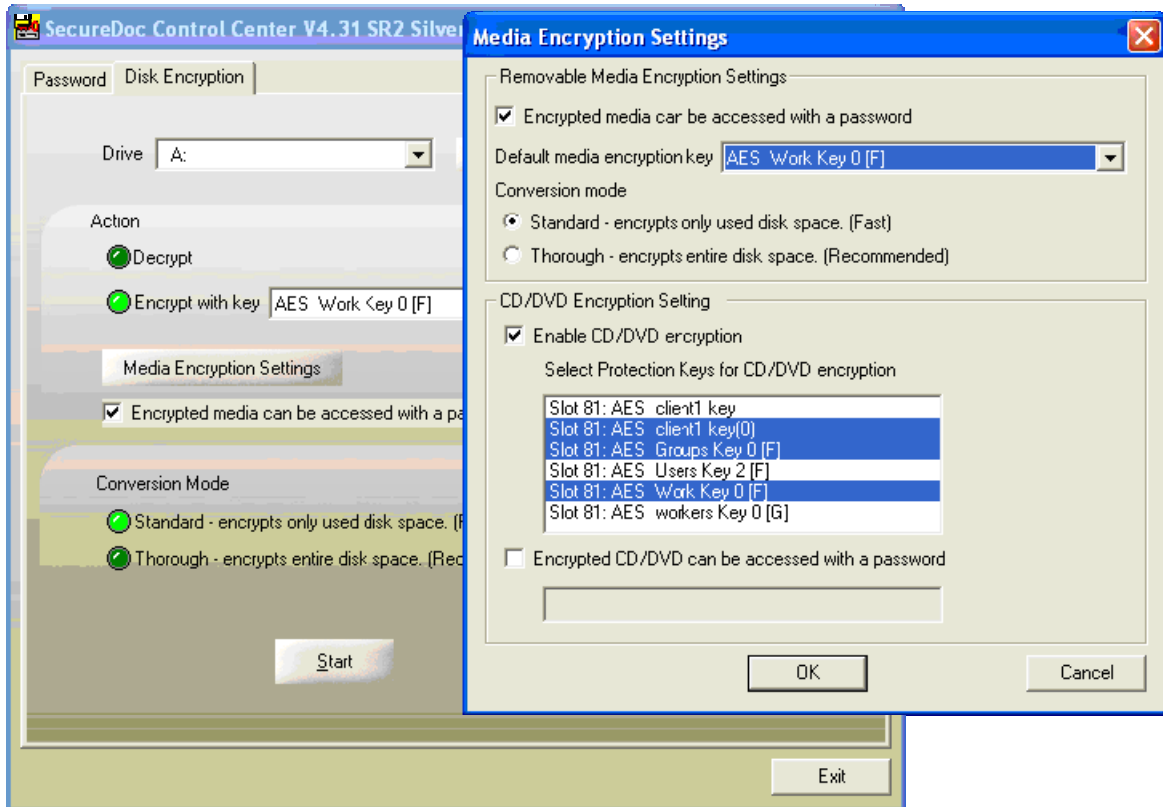
Alternativ zu einem Passwort kann hier auch eine starke Authentisierung mittels Smartcard oder Token verwendet werden.

Gleich nach dem ersten Start nach der Installation sollte der Benutzer 2 Dinge erledigen (entsprechend der Vorgaben in seinem Profil), er muss sein Anfangspasswort ändern und er muss seine Identifizierungsantworten für die Passwortwiederherstellung angeben. (Und sollte der Benutzer auch einen „Personal Firewall“ laufen haben – Windows XP - dann sollte er dem Firewall auch „**unblock**“ angeben, wenn er dazu aufgefordert wird. Und so sieht das aus:



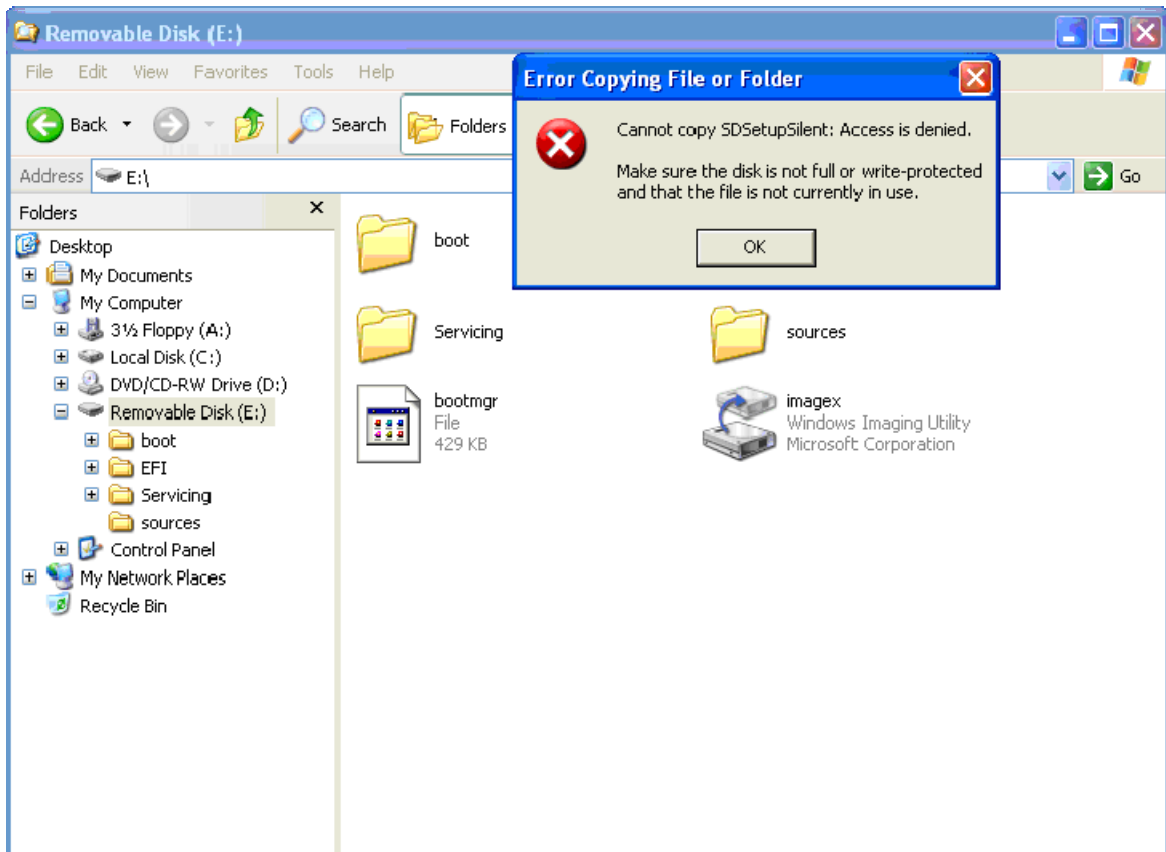
Das wars auch schon....

In unserem Falle hat der Benutzer das Recht, die Einstellungen bei der Verschlüsselung der Medien selbst zu ändern und Medien mit Zugriff für von ihm selbst benannten anderen Benutzern und Gruppen zu erstellen (nur bei wirklich versierten Benutzern zu empfehlen :-)

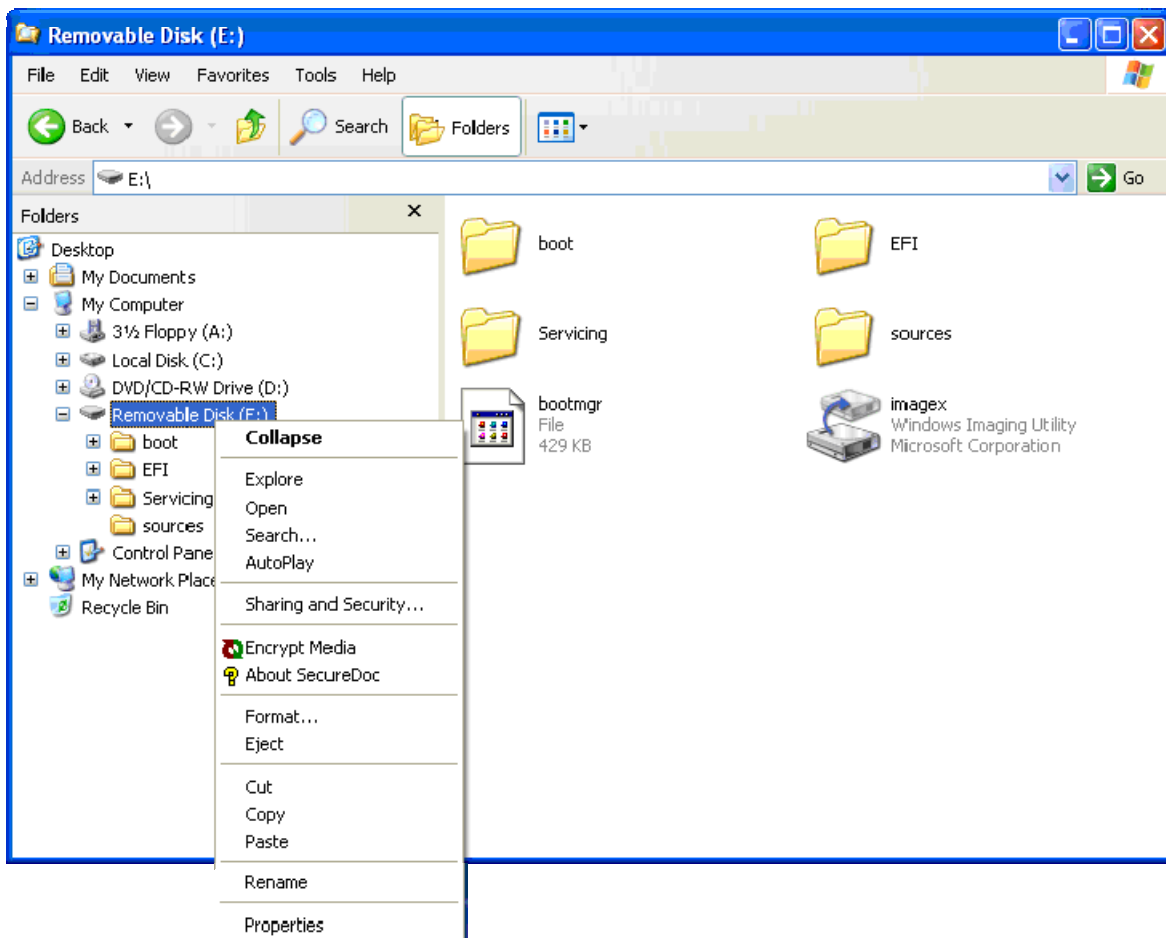


Wechselmedien

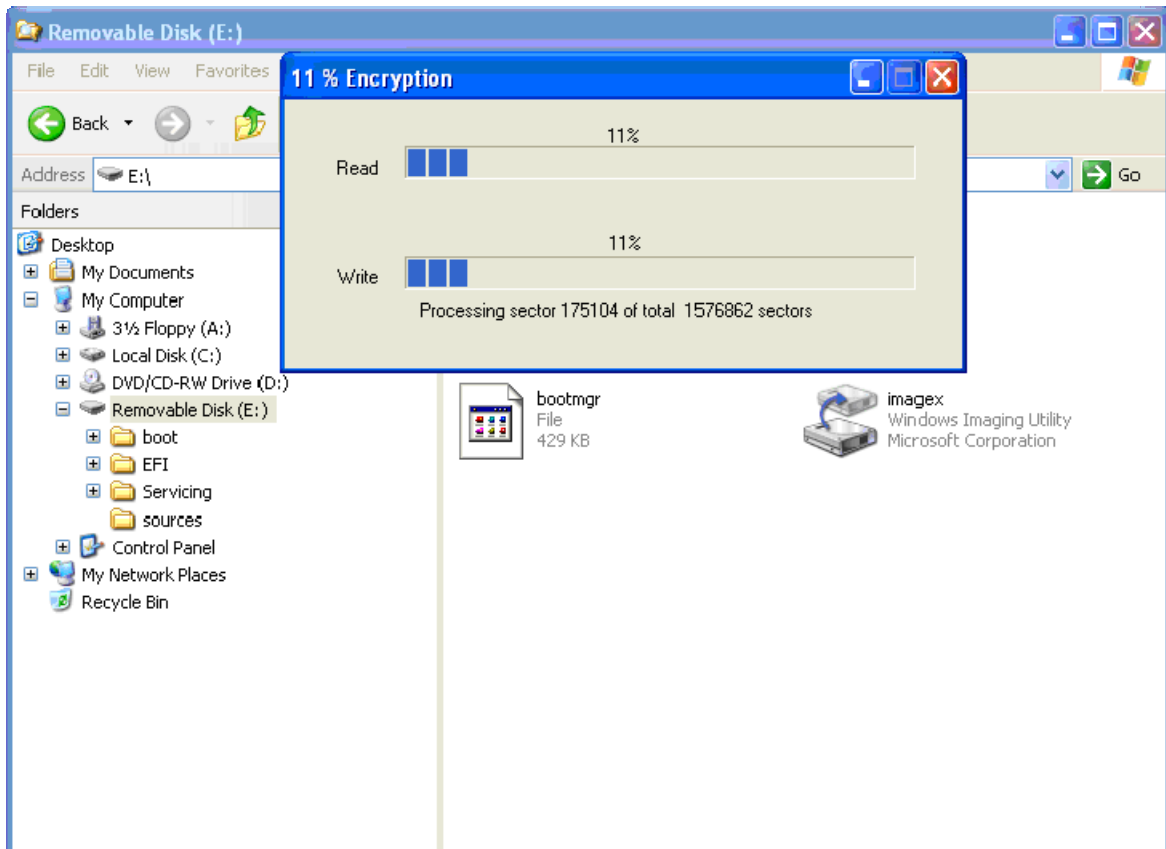
Wenn ein Benutzer ein Wechselmedium in Betrieb nimmt, in unserem Falle ein USB Stick, kann er es nur in dem Maße nutzen, wie es im SES Profil gestattet ist. In unserem Falle ist es erlaubt, unverschlüsselte Inhalte zu lesen, aber nicht auf unverschlüsselte Medien zu schreiben.



Wenn der Benutzer das Medium auch zum Schreiben nutzen will, etwa um damit Daten innerhalb seiner Organisation auszutauschen, so muss er das Medium zuerst verschlüsseln.



Nach der Bestätigung (und optional der Wahl eines Passwortes – siehe Profil) beginnt SecureDoc das Medium zu verschlüsseln. Danach ist das Medium nur mehr auf jenen Computern möglich, an denen ein Benutzer der berechtigten Gruppe angemeldet ist



Wenn in einer Organisation ein so hoher Bedarf an Sicherheit gegeben ist, dass nicht auf unverschlüsselte Medien geschrieben werden darf, so empfiehlt es sich um den Helpdesk zu entlasten, dass

- die Benutzer nicht die Erlaubnis haben, die Verschlüsselungseinstellungen zu ändern und
- verschlüsselte Medien für Abteilungen und/oder Standorte von der IT Abteilung oder dem Helpdesk vorbereitet und dann ausgegeben werden.

Einerseits ist es eine stete Fehlerquelle, wenn Benutzer selbst für Gruppen verschlüsseln (Irrtümer und anschließende Anrufe beim Helpdesk oder sogar Sicherheitslücken sind vorprogrammiert) und andererseits kann es durchaus mal längere Zeit in Anspruch nehmen, einen großen aber langsamen Stick zu verschlüsseln.

Passwort vergessen?

In den Einstellungen des Profiles legt man fest, nach wie vielen Fehlversuchen beim Startpasswort ein Computer gesperrt wird. Hier wird nicht der Computerstart selbst gesperrt, sondern der Zugriff auf das Keyfile, und damit kann die Festplatte nicht mehr genutzt werden. In diesem Falle muss ein Prozess vorbereitet werden, nach dem ein Benutzer / Helpdesk Mitarbeiter den Computer rasch wieder betriebsbereit gemacht werden kann (SecureDoc Enterprise Server erlaubt auch hier eine genaue Anpassung an die Sicherheitsbedürfnisse und die Struktur der Organisation)

Beispiel:

Spielen wir einmal einen Fall gemeinsam durch:

Ein Benutzer versucht sich an seinem Computer anzumelden und glaubt, sich an ein (leider falsches) Passwort zu erinnern:



Auch der freundlicherweise aktive „password hint“ nützt ihm diesmal nichts.

Nach 3 Versuchen muss er das System neu starten und kann erneut versuchen sich zu erinnern, bis er die vom Administrator eingestellte maximale Zahl (hier 5) an Versuchen erreicht hat.



Nun geht nichts mehr, das Keyfile ist gesperrt und erlaubt keine weiteren Rateversuche.

In unserer Beispielininstallation ist das **Online Recovery Tool** verfügbar. Unser Benutzer benötigt nun Schreibzeug und einen noch funktionierenden Computer (etwa den eines Arbeitskollegen) der Zugriff auf die Webseite des SES hat.

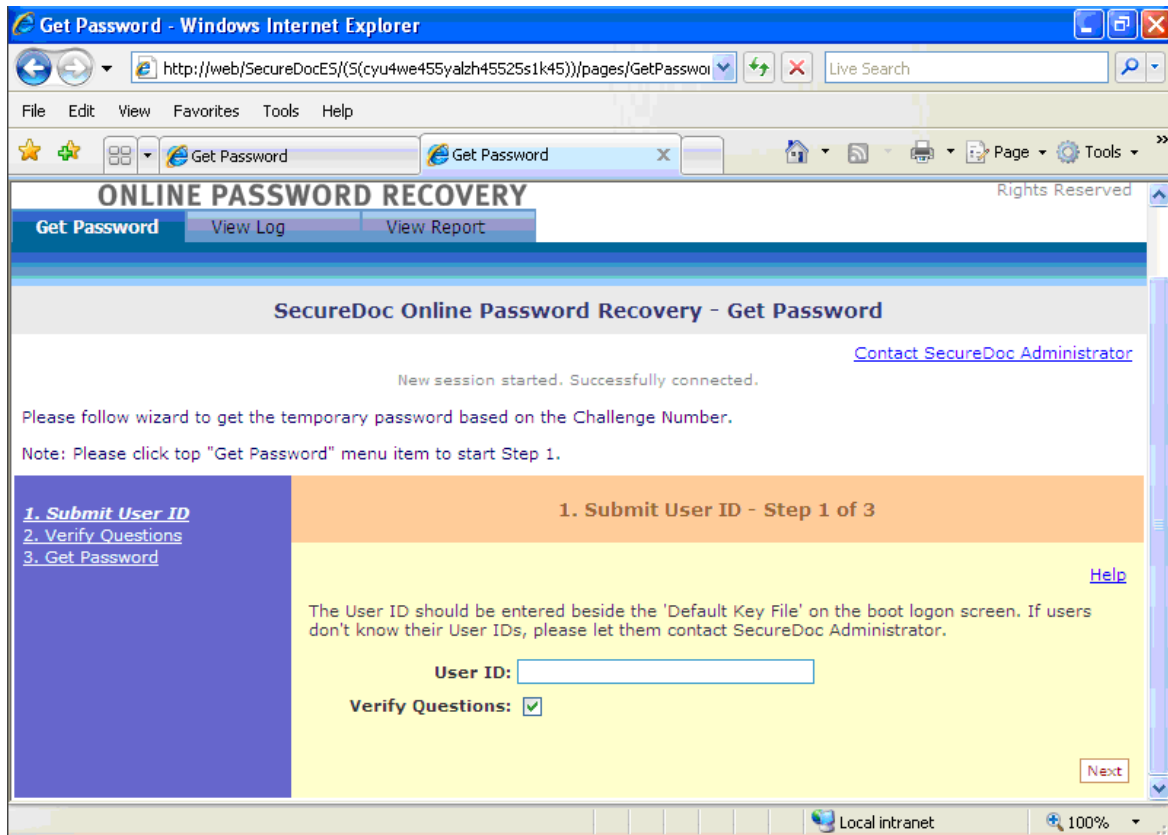
Er startet den Computer neu und drückt anstelle des Logon die Taste **F8**



Die „Challenge“ des Computers muss der Benutzer sich nun merken oder aufschreiben. Damit kann er sich nun zu einem funktionierenden Computer begeben oder einen Kollegen anrufen, der zu einem funktionierenden Computer Zugriff hat.

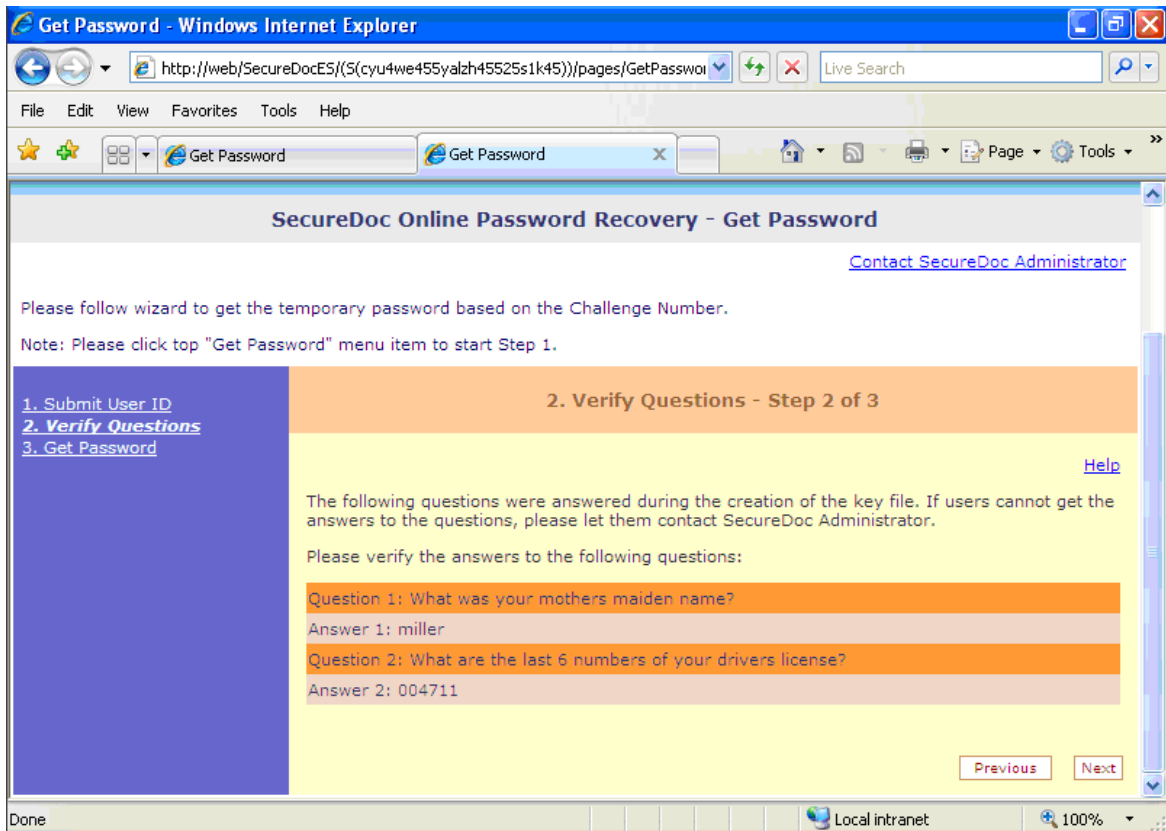
Dort wird die OPR (online password recovery) website gestartet:

<http://hostname/securedoces/home.aspx>



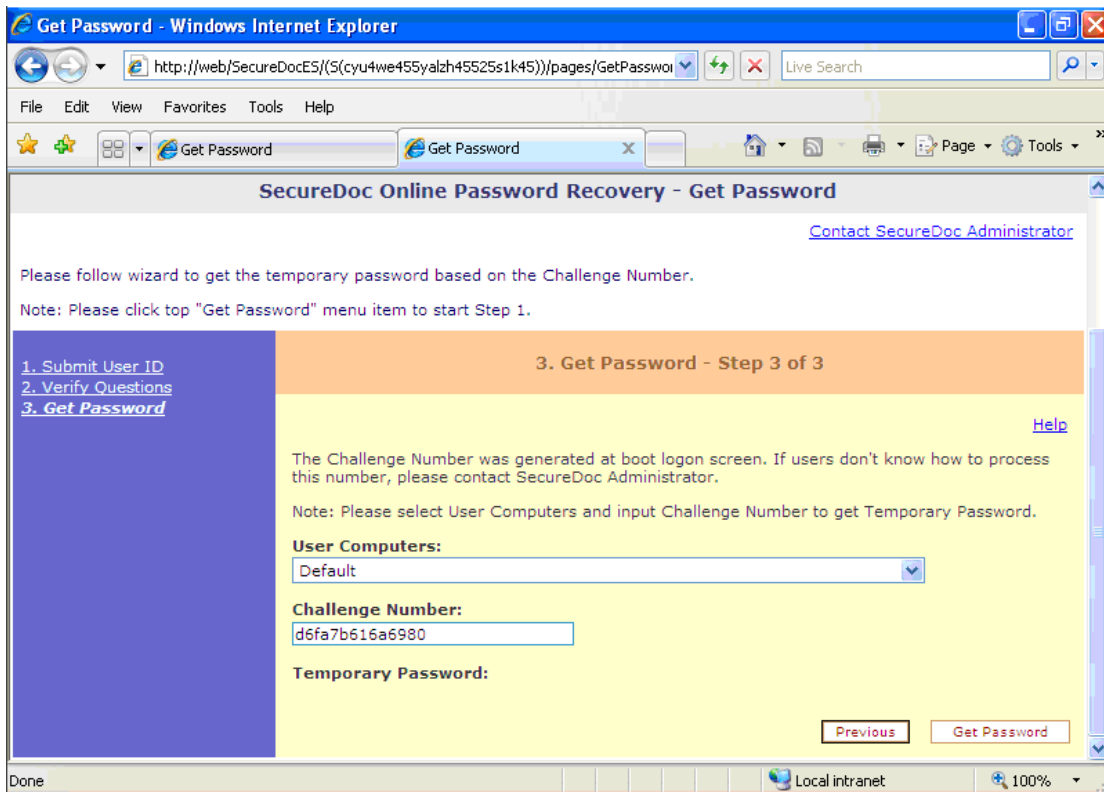
Nach der Eingabe der SES UserID (in unserem Falle wurde das Domain Konto als Vorlage gewählt, also sind UserID uns AD Anmeldekonto identisch) werden dem Kollegen oder Helpdesk Techniker die Identifizierungsfragen und deren Antworten präsentiert.

Anhand der Antworten kann der Kollege oder Helpdesk Techniker den hilfeschenden Benutzer identifizieren.

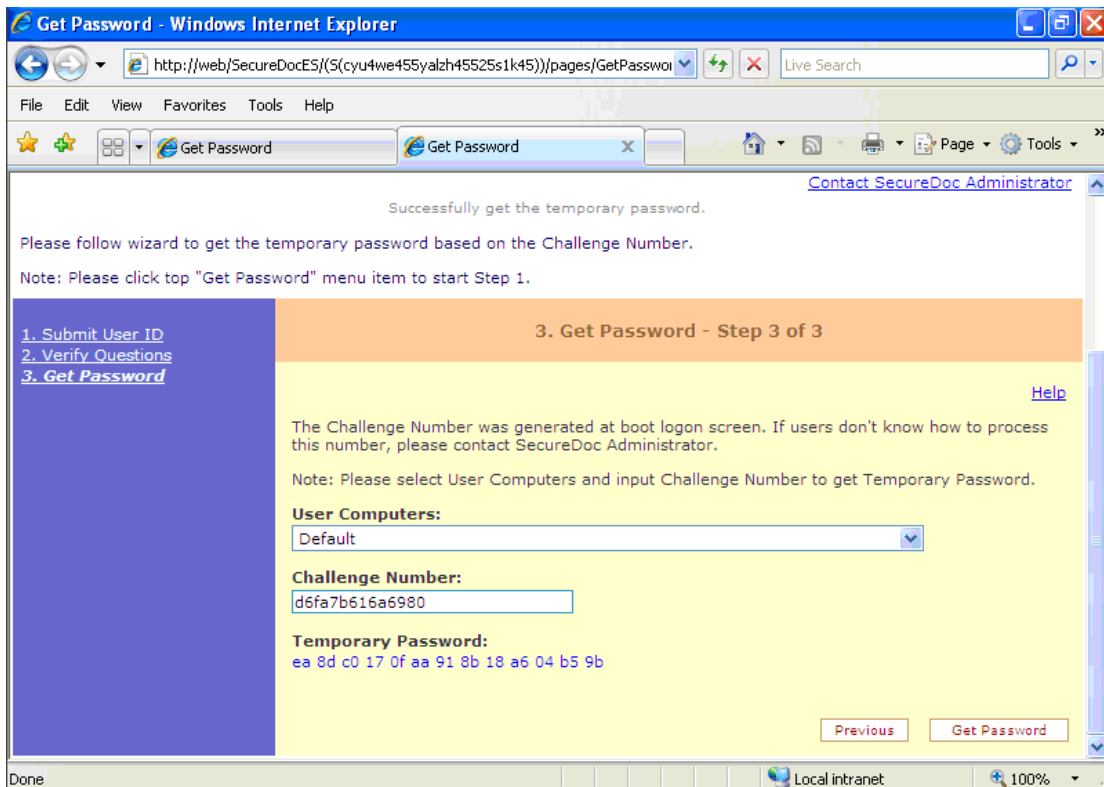


Er vergleicht die vom Benutzer gegebenen Antworten mit denen aus der Datenbank, stimmen sie überein, so kann er davon ausgehen, daß der Anrufer tatsächlich der ist, für den er sich ausgegeben hat:

Dann kann die Challenge eingegeben



.... und die „Response“ dem Benutzer übermittelt werden.....



Damit kann der Benutzer nun seinen Computer starten.

Alternativen:

- Ein Helpdesk Techniker, der über die Smartcard oder das Token des für diesen Standort oder die Gruppe an Computern festgelegten Recovery Admins verfügt, meldet sich persönlich am Computer an und entsperrt damit das Keyfile.
- Der Benutzer verwendet das alternative Logon mittels der Identifizierungsfragen, bevor er seine 5 Versuche aufgebraucht hat und ändert dann sein Passwort. Er drückt anstelle des Logon **F9**. Das ist auch eine gute Alternative, wenn er seine Smartcard vergessen hat und die Organisation eine alternative Anmeldung mittels Benutzername und Passwort erlaubt.

Tip an den Administrator zur IT Sicherheit: **bevor** wir die Anmelde und Recovery Optionen festlegen, besprechen wir uns noch einmal mit dem **Sicherheitsverantwortlichen** und arbeiten die Überlegungen in das Support Konzept ein. Ein Online Password Recovery, das von Benutzern selbstständig verwendet werden darf (Permissions auf Domain User oder Anonymous Access) kann in Kombination mit der alternativen Anmeldung über Identifizierungsfragen eine schwere Sicherheitslücke darstellen. Unbefugte mit Zugriff auf diese Website können die Fragen und die Antworten der Benutzer auslesen und damit den Schutz des Computers umgehen.

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
www.cryptas.com