

SECURITY : CONSULTING : SHOP : INTEGRATION



**Signatory:** cryptoshop.com - Cryptas it-Security GmbH  
**Time:** UTC 2008-01-24, 11:18:29  
**ID:** 73 EA 3B C9 2A 11 4E FA 20 94  
42 71 64 06 83 9A A3 0C 98 84  
**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

## Allgemeine Funktion

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 zur Funktion von WinMagic SecureDoc Enterprise Server (SES)

Der SecureDoc Enterprise Server von Winmagic ist eine leistungsstarke Anwendung zum Schutz der vertraulichen Informationen eines Unternehmens durch Verschlüsselung. Die hervorstechendsten Eigenschaften des SecureDoc Enterprise Servers sind seine hohe Integration in die Microsoft Windows Umgebung (Active Directory, Windows PKI, MS-SQL), seine Skalierbarkeit, die einfache Verwaltung und nicht zuletzt der besonders gute Schutz der Daten durch stärkste Verschlüsselung und der Unterstützung von starker Authentisierung.

Starke Verschlüsselung:

SES verwendet AES 256 („Advanced Encryption Standard“- ein Algorithmus mit 256 Bit Verschlüsselung) zur symmetrischen Verschlüsselung der Daten. Darüber hinaus werden diese symmetrischen AES Schlüssel wiederum mit einem asymmetrischen Schlüssel (digitale Zertifikate!) geschützt abgelegt. Nur der Besitzer des geheimen (privaten) Schlüssels hat Zugriff auf den „Schlüsselbund“ mit den symmetrischen Schlüsseln. Diese Zertifikate können wahlweise von einer vorhandenen PKI (Beispiel: Microsoft Windows 2000 Server oder jünger) oder von der im SES integrierten Certification Authority ausgestellt werden.

Starke Authentisierung:

Anstelle der Benutzung von Passwörtern zum Zugriff auf den „Schlüsselbund“ (schwache Authentisierung) können optional auch fortgeschrittene Technologien, wie etwa Smartcards oder Smart-Tokens, genutzt werden. In diesem Falle wird der private Schlüssel des Benutzers (zum Zugriff auf den „Schlüsselbund“) auf der Karte oder dem Token des Benutzers mitgenommen. Es bleibt keine angreifbare Information auf dem Computer des Benutzers zurück (starke Authentisierung)

„Etwas, das man hat (Token oder Smartcard) UND etwas, das man weiß (Pin)“

Einsatzmöglichkeiten:

SecureDoc Enterprise Server ermöglicht die Verwaltung der Funktionalitäten von SecureDoc in einer professionellen Umgebung. Hierzu zählen:

- Festplattenverschlüsselung von Client Computern und Servern. Wahlweise können die gesamten Festplatten der Computer oder einzelne Partitionen darauf verschlüsselt werden. Wenn man sich dazu entschließt, die Festplatte eines Computers zu verschlüsseln, muss der Benutzer sich VOR dem Booten des Computers authentisieren (Preboot Authentication)
- „Container encryption“ - es besteht die Möglichkeit, verschlüsselte Bereiche auf einer Partition einzurichten, die vom Betriebssystem als separates „Laufwerk“ behandelt werden.
- „File and folder encryption“ - Einzelne Dateien und Ordner auf Festplatten, Medien oder am Server-„share“ können für einzelne Personen oder Gruppen von Personen verschlüsselt werden.
- „Media encryption“ – Die Verschlüsselung des Inhaltes von CD/DVD, USB Speichergeräten oder sogar Disketten kann wahlweise angeboten oder erzwungen werden.
- „Selfextractor“ – Im speziellen Falle kann auch mal eine Datei oder ein Ordner verschlüsselt an externe Empfänger übertragen werden. In diesem Falle sind die Schlüssel zum Zugriff auf die Datei zwar nur durch ein Passwort geschützt, aber der Empfänger braucht nicht Mitglied der eigenen Organisation zu sein. Er benötigt nur den SD Selfextractor, der allerdings frei erhältlich ist.

#### Skalierbarkeit:

SecureDoc Enterprise Server genügt auch den Anforderungen einer großen Organisation.

- Ausfallsicherheit: die Komponenten des SES können mehrfach vorhanden sein
- SES unterstützt sowohl eine Netzwerkarchitektur mit mehreren Standorten, als auch sogenannte „Offline Clients“ (Computer, die niemals Verbindung zum Netzwerk der Organisation haben).
- Darüber hinaus können nicht nur Daten auf Client Computern und Servern, sondern auch auf PDAs geschützt werden.
- Die Betreiber einer IT Umgebung können frei entscheiden, welche Funktionalitäten welchen Gruppen von Computern zur Verfügung gestellt werden. So kann flexibel auf den Bedarf von Standorten, Benutzer und Computerklassen und deren Rollen im Unternehmen reagiert werden. (Ein Standgerät im „Headoffice“ ist möglicherweise ganz anderen Bedrohungen ausgesetzt als das Notebook eines Feldtechnikers oder eine CNC Maschine am Band und benötigt daher einen gänzlich anderen Satz an Funktionalitäten)

#### Verwaltung des Zugriffes auf verschlüsselte Informationen:

Der Zugriff auf Ressourcen, verschlüsselte Daten und verschlüsselte Computer, wird von einer „Management Konsole“ von dazu bestimmten Administratoren verwaltet. Dazu können Benutzer einer oder mehreren Gruppen und Containern zugeordnet werden, die jeweils für den Zugriff auf einzelne Ressourcen oder Geräte stehen. Benutzer und Gruppen können auch von Microsoft Active Directory (AD) übernommen und mit dem AD synchronisiert werden. Die „Keyfiles“ auf den einzelnen Computern (Schlüsselbund) werden automatisch auf den neuesten Stand gebracht, wenn in der Management Konsole ein Schlüssel hinzugefügt oder davon entfernt wird. Dem Helpdesk steht außerdem ein benutzerfreundliches und dennoch sicheres Password Recovery/ Key Recovery Verfahren zur Verfügung.

#### Verwaltung der Client Einstellungen:

Berechtigungen, angebotene Funktionalitäten und andere clientspezifische Einstellungen werden von SecureDoc Enterprise Server in Profilen definiert. Diese Einstellungen werden automatisch an die dafür vorgesehenen Client Computer verteilt, sobald sich eine Einstellung ändert. So lassen sich sowohl einzelne Computer, als auch ganze Gruppen von Geräten mit ähnlichen Bedürfnissen bequem verwalten.

#### Integration in die Microsoft Windows Umgebung:

- SES nutzt MS SQL als Datenbank Server
- SES kann Active Directory als Quelle für Benutzerkonten, Gruppen und Container, sowie für die Verwaltungsstruktur nutzen
- SES kann die von der MS PKI erstellten Zertifikate nutzen
- SES kann die von Windows angebotene Smartcard Authentisierung nutzen
- Die von SecureDoc für die einzelnen Client Computer vorbereiteten SecureDoc Installationspakete können von MS SMS und seinem Nachfolger automatisch verteilt werden.

#### Unterstützung anderer Umgebungen:

- SecureDoc ist auch auf Linux Systemen nutzbar
- SES kann Benutzerkonten und Gruppen aus jedem verfügbaren LDAP Verzeichnis importieren
- SES kann die Zertifikate von jeder X.509V3 kompatiblen PKI nutzen
- Securedoc Installationspakete können von jedem Softwareverteilungssystem auf den Client Computern installiert werden.

## Komponenten des SecureDoc Enterprise Servers (SES)

SecureDoc Enterprise Server besteht aus mindestens 3 (optional 5) Komponenten

Im Hintergrund befinden sich:

- Die SES Datenbank
- Die SES Management Konsole

Im Vordergrund sind Verbindungsdienste sichtbar:

- SD Connex
- SD Active Directory Sync (optional)
- Online Password Recovery (optional)

Die SES Datenbank:

SecureDoc Enterprise Server legt alle Informationen, Gruppenzugehörigkeiten, Eigenschaften, Passworte und Zugriffsschlüssel in einer verschlüsselten Datenbank ab. Diese Datenbank kann auf jedem existierenden SQL Server als zusätzliche Datenbank oder auch in einer Instanz einer SQL Desktop Edition (SQL 2000 MSDE oder SQL 2005 Express Edition) laufen. Administrative Rechte sind auf dem SQL Server nach Erstellung der Datenbank nicht mehr notwendig.

Die SES Management Konsole:

Die Management Konsole dient dem Zugriff auf und der Darstellung der verschlüsselten Inhalte der Datenbank. In Ihr werden Einstellungen gesetzt, Schlüssel und Benutzer verwaltet, Installationspakete vorbereitet und Ereignisse nachvollzogen. Sie kann auf der Workstation des zuständigen SES Administrators installiert werden. Es können mehrere Konsolen auf eine Datenbank zugreifen.

SD Connex:

Das ist der Kommunikationsdienst von SecureDoc Enterprise Server. SD Connex hält die Verbindung zwischen den Client Computern und der Datenbank. Er muss allen betroffenen Clients der Organisation sichtbar sein. In großen Organisationen können mehrere SD Connex Dienste vorhanden sein. Offline Computer kommunizieren mit der Datenbank über Dateien, die per Email, CD, oder USB Medien ausgetauscht werden können.

SD Active Directory Sync (optional):

Dieser Dienst synchronisiert Benutzerkonten, Gruppen und Container mit Microsoft Active Directory. Änderungen im AD werden automatisch in die SES Datenbank übernommen. Umgekehrt werden Änderungen, die direkt in der SES Datenbank getätigt werden, nicht ins AD zurückgeschrieben

Online Password Recovery (optional):

Das OPR ist ein Webinterface, das es dem Helpdesk und auch den Benutzern selbst ermöglicht, vergessene Passworte oder gesperrte Computer auf sicherem Wege wiederherzustellen bzw. zu entsperren, ohne dabei den SES Admin erreichen zu müssen.

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)