Exchange 2000 Key Management Server Migration to a Windows 2003 CA

Written by Marc Grote
MCP, MCP+I, MCSA 2K/2K3, MCSA-S-E 2K, MCSE NT4/2K/2K3, MCSE-S 2K, MCT, CNA, CCNA, CCA, CCSA
mailto:grotem@it-training-grote.de

Abstract

Exchange 2003 uses the Windows Server 2003 PKI architecture to provide secure e-mail services for Exchange users. Exchange 2000 KMS is no more supported. The Windows 2003 Enterprise CA provides central key archiving and recovery.

This article explains in high level steps how to migrate an Exchange 2000 KMS database to a Windows Server 2003 CA.

This article is based on Windows 2003 Enterprise Edition (Build 3790) and Exchange 2000 Enterprise Service Pack 3.

Reference: Exchange 2000 Online help

Introduction

Exchange 2000 Administrators must use the Key Management Server database to offer secure e-mail services for Exchange users with Outlook Clients.

Windows 2000 offers its own Public Key Infrastructure (PKI) which provides services to issue certificates (e-mail certificates, EFS-certificates and so on).

You as an Administrator have to manage both services which are more time intensive.

With Exchange 2003 there is no separate Key Management Database. Exchange 2003 uses the Windows 2003 Enterprise CA capabilities to offer secure e-mail services.

Export of the Exchange 2000 KMS database

Before we export the KMS database we have to import a certificate from the Windows Server 2003 CA which will be used to encrypt the exported KMS database. The steps to export a certificate from a Windows 2003 CA and to import this certificate into the certificate store of the Exchange Server are not part of this article.

To start the export - Start Exchange System Manager and go to “Advanced Security” – Key Manager and select “All Tasks” – “Export Users”

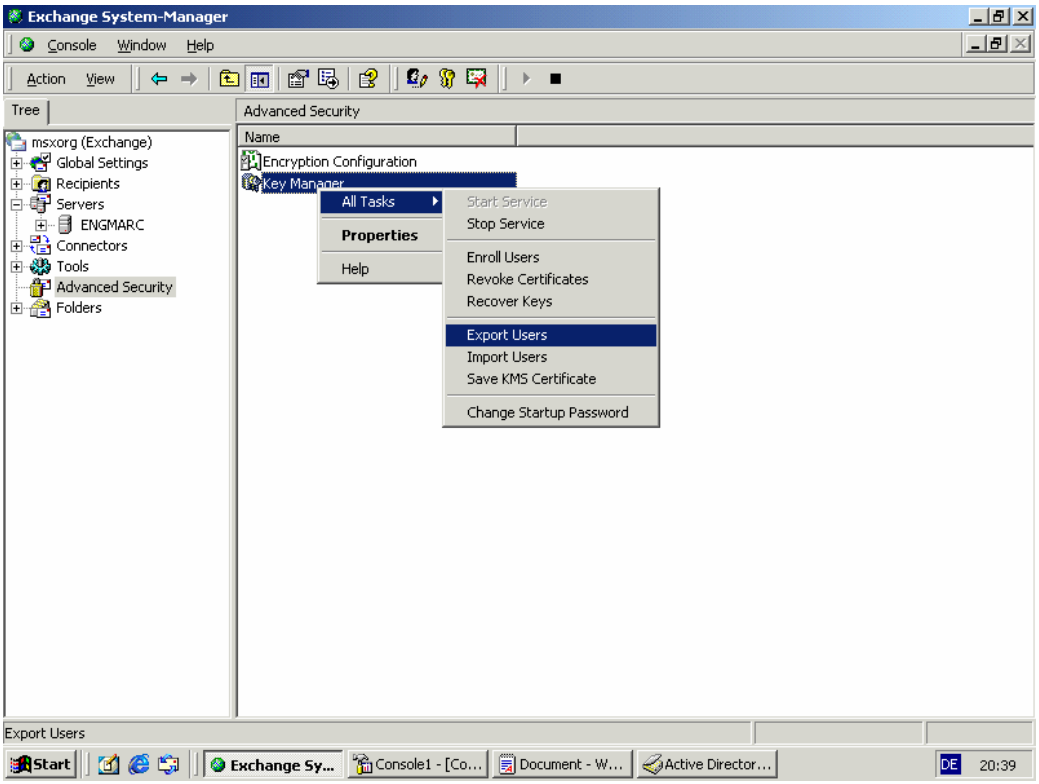

Figure 1: Export the KMS users in Exchange 2000 System Manager

Browse the path to the exported Windows 2003 CA certificate. This certificate is used to encrypt the exported KMS database.

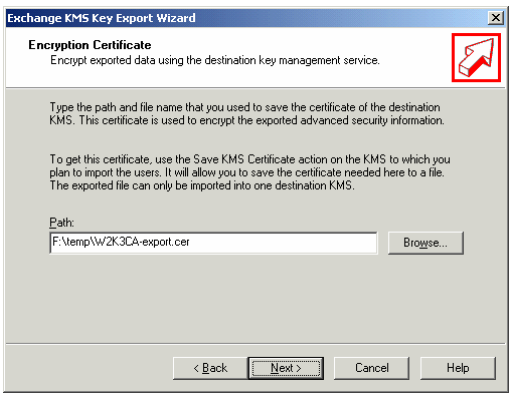

Figure 2: Specify the exported Windows Server 2003 certificate

For security reasons enter the first eight characters from the thumbprint from the Windows 2003 CA certificate.

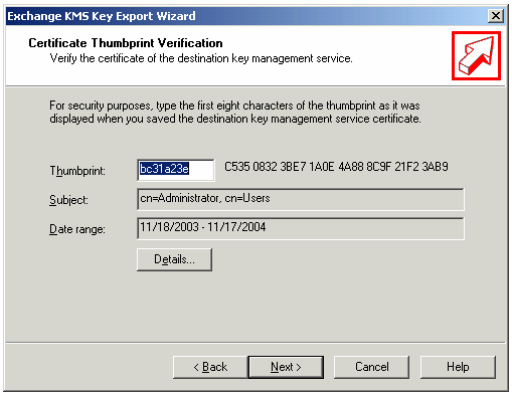

Figure 3: Enter the first eight characters of the thumbprint

Specify the name of the file for the exported KMS database. The default path is \EXCHSRVR\KMSDATA

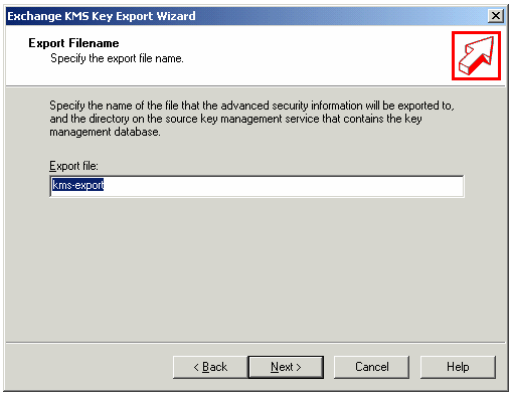

Figure 4: Enter the name of the export file

Select the users to export from the KMS database

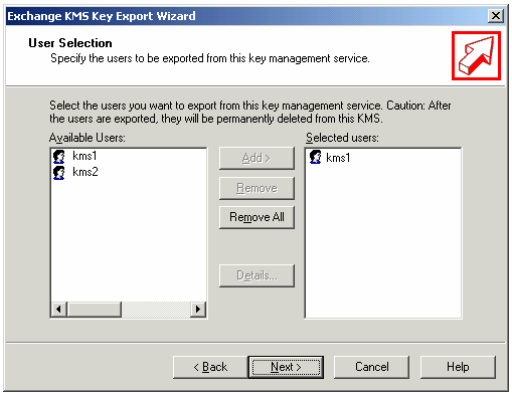

Figure 5: Export the KMS users in Exchange 2000 System Manager

Congratulation: You have successfully exported the selected users.

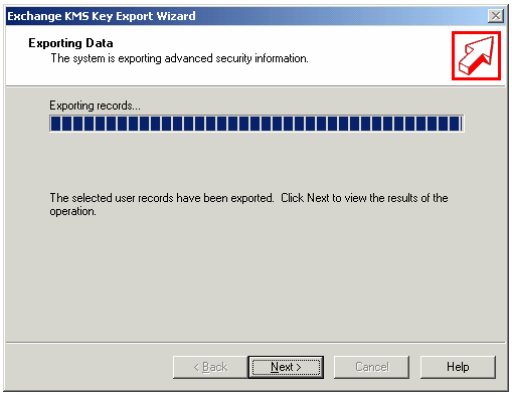

Figure 6: See the process of exporting the users

Import of the exported KMS database from KMS to Windows 2003 CA

Before we can import the KMS database into the Windows 2003 CA store, we must enable the Windows 2003 CA to archive private keys. To do this we have to issue a Key Recovery Agent certificate for the account used to migrate the KMS database and to enable key archiving under “Recovery Agents” in the Certificate Authority SnapIn.

The high level steps to this are:

- Issue a “Key Recovery Agent” certificate Template (Start – All Programs - Administrative Tools – Certification Authority – Certificate Templates – New – “Certificate template to issue”)
- Create a custom MMC – and add the Certificate SnapIn for the User Account that will migrate the KMS database
- Specify the Key Recovery Agent certificate under the properties of the Certificate Authority under “Recovery Agents”.

Enable the CA for foreign key import

Before we can import the KMS database into the certificate store of the Windows 2003 CA we have to allow the import of foreign certificates.

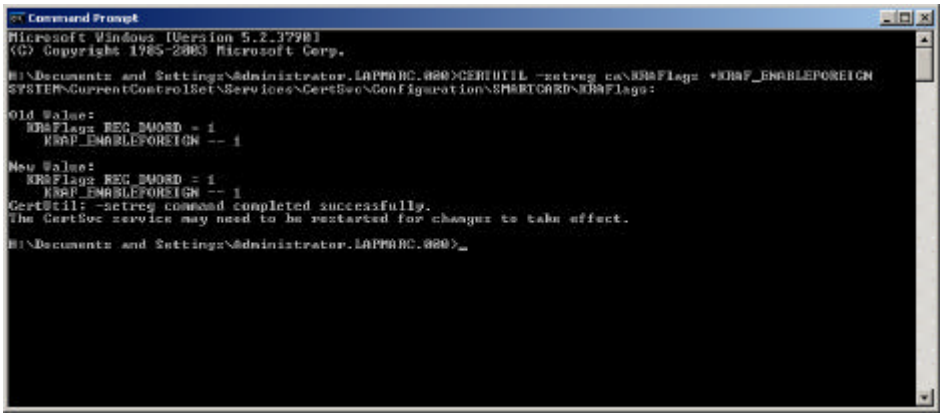

Figure 7: Enable the CA to import foreign certificates

Now we have to import the exported KMS database with CERTUTIL:

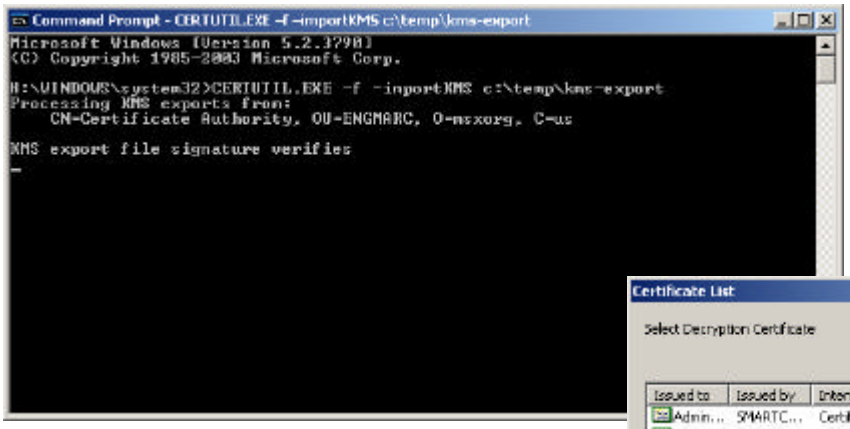

Figure 8: Import the exported KMS database

Select the certificate which we have used to export the KMS database

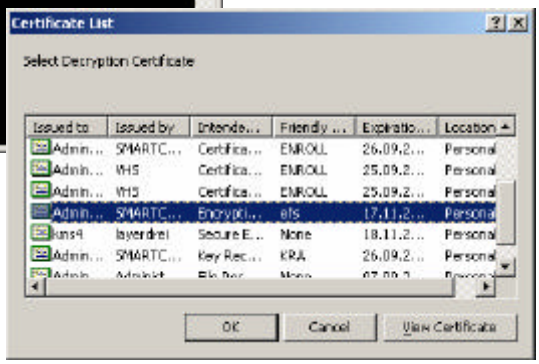

Figure 9: Select the certificate to encrypt the database

Import the KMS database into the Windows 2003 CA with CERTUTIL

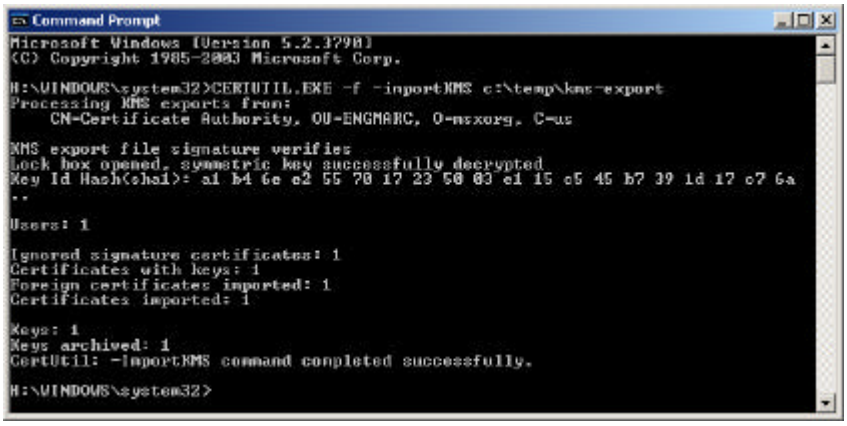

Figure 10: Import the KMS database

Key recovery

Run the Tool KRT.EXE from the Windows Server 2003 Resource Kit to perform a GUI recover of the selected certificate. You have to specify the serial number of the certificate in the Value field to recover the certificate. Next click “Recover” to recover the certificate

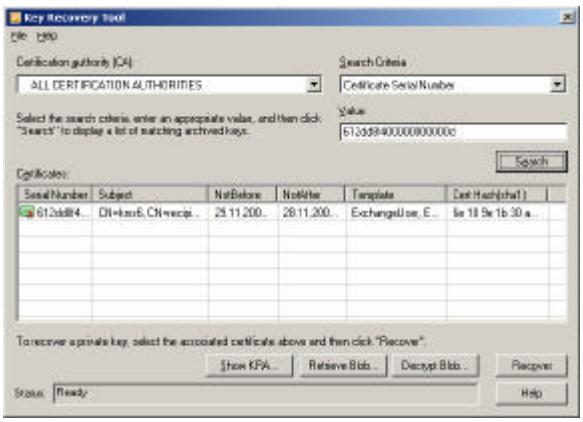

Figure 11: The Key Recovery Tool (KRT)
Choose the path to save the file and select a password to protect the recovered .PFX file. The Prefix .PFX shows that the private key is included in this file.

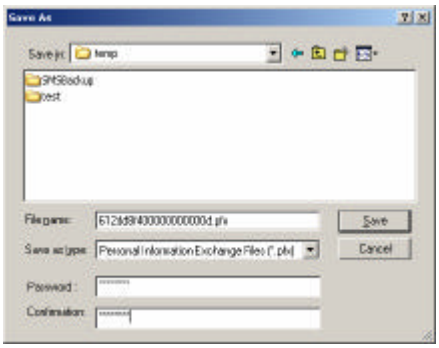

Figure 12: Specify the path to the .PFX file

Congratulation. You have successfully recovered the certificate

Figure 13: Import the exported KMS database

Conclusion

The integration of the Key Management Services from Exchange 2000 into the Windows 2003 Enterprise CA is the next logical step for the Exchange 2003 deployment. With this constellation you can use the full power of the Windows 2003 Enterprise CA.

Related Links

Microsoft Exchange 2003 Homepage
http://www.microsoft.com/exchange
Windows 2003 Homepage
http://www.microsoft.com/windows2003