

Exchange 2003 – Key Archiving and Recovery

Written by Marc Grote - <mailto:grotem@it-training-grote.de>

Abstract

In this article I will show you how to setup a Windows 2003 Enterprise CA for archiving and recovering keys for e-mail encryption.

Let`s begin

Beginning with Windows Server 2003, Microsoft has enhanced its own PKI-solution with several new features like:

- ? Key Archiving and Recovery
- ? Role Separation
- ? Qualified subordination
- ? Version 2 Certificate Templates

To get these entire wonderful new features, you must buy Windows Server 2003 Enterprise, because the Standard Version of Windows Server 2003 doesn't offer these features.

One of the biggest enhancements is the Key Archiving and Recovery feature. With this feature, every certificate (the private key) issued by a Windows 2003 Enterprise CA will be archived at the CA. Key Archiving is not available for certificates with e-mail signature only purpose.

In this article we will issue an e-Mail certificate for the user MSEXCHANGEORG and assume that this user has lost his e-mail certificate. With the help of a Key Recovery Agent (KRA) and the Windows Server 2003 Resource Kit Utility KRT.EXE we will recover this certificate.

This article will give you only a high level overview about the entire process. If you have more questions, follow the links at the end of this article.

Key Archiving and Recovery requires multiples steps:

- ? Enabling the Key Recovery Agent
- ? Enable the CA for key archiving
- ? Issue e-mail certificates to users
- ? Recover e-mail certificates (KRT and CERTUTIL)

Enabling the Key Recovery Agent

First, we need to enable a Key Recovery Agent. A Key Recovery Agent is a highly trusted person which is responsible to recover lost or damaged archived certificates for users. We must issue a Key Recovery Agent certificate for this user. To do this:

- ? Start the Windows 2003 CA console
- ? Issue a new template named Key Recovery Agent
- ? Request this certificate for the user who becomes the Key Recovery Agent
- ? Manually Issue the Key Recovery Agent Certificate at the CA

Figure 1 shows the issued Key Recovery Agent Certificate for the user Administrator.

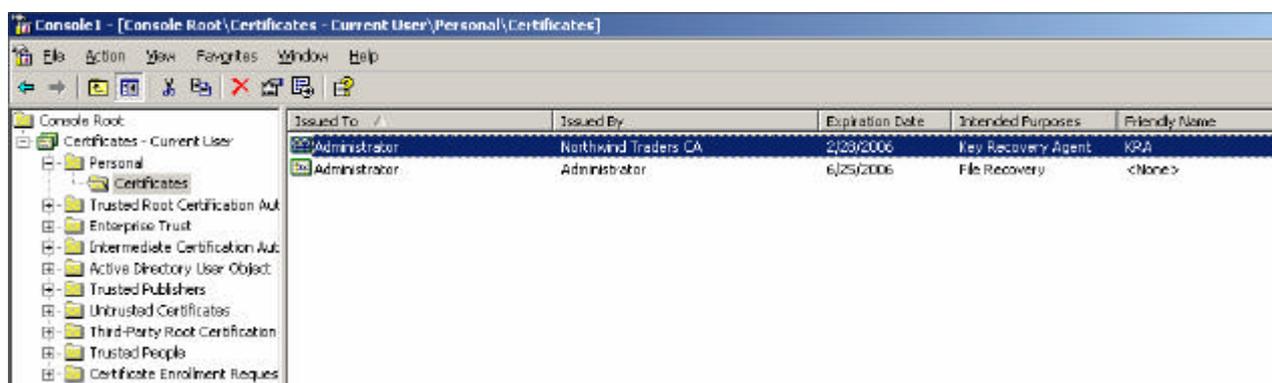


Figure 1: Issued Key Recovery Agent certificate

Important:

The Windows 2003 CA will not automatically issue this certificate to the user who requests the Key Recovery Agent certificate. The CA Administrator must manually Issue the certificate in the Microsoft CA MMC under *Pending Requests*.

Enable the CA for key archiving

Now it is time to enable the CA for Key Archiving. Start the Microsoft CA MMC and navigate to the CA properties – *Recovery Agents*.

Because Key Recovery is a very security sensible process, you can specify how many Recovery Agents are required to Archive keys. Click *Add* to import the Key Recovery Agent certificate. Click *OK* and restart the CA service.

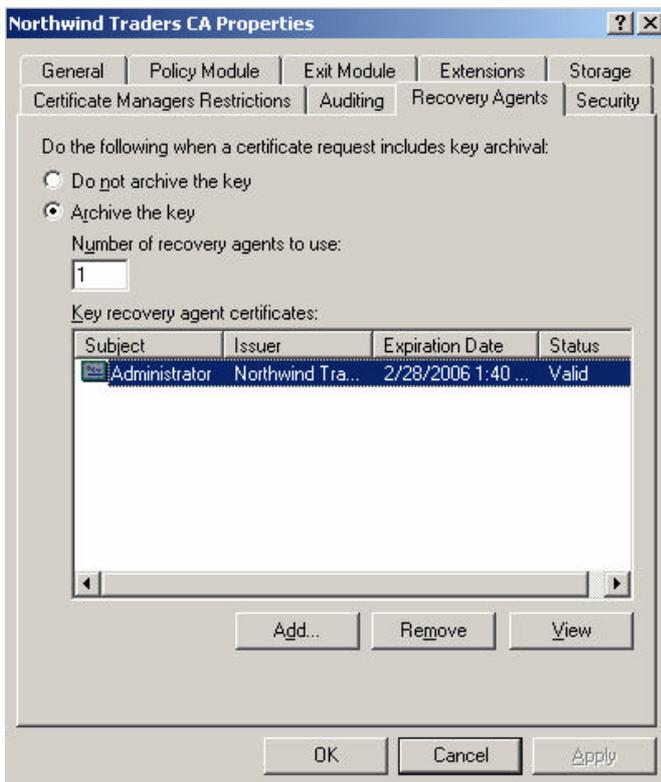


Figure 2: Enable the CA for Key archiving

Now it is time to duplicate an e-Mail Certificate Template at the Windows 2003 CA. The question is why? The default e-mail Certificate Template doesn't allow the archiving of the subject's private key. Start the Microsoft CA MMC, navigate to *Certificate Templates* and rightclick *Manage* – Select the *Exchange User Certificate Template* and click *Duplicate* and name the new template. In the Request Handling section click *Archive subject's encryption private key*.

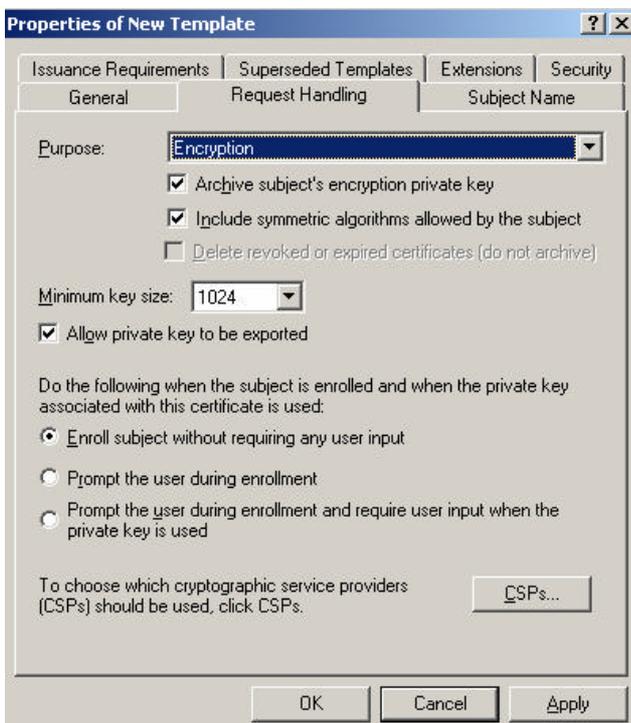


Figure 3: Enable Key Archiving in the Certificate Template

The new Certificate Template (Exchange User (KeyARC) is now ready to issue certificates and to archive keys.

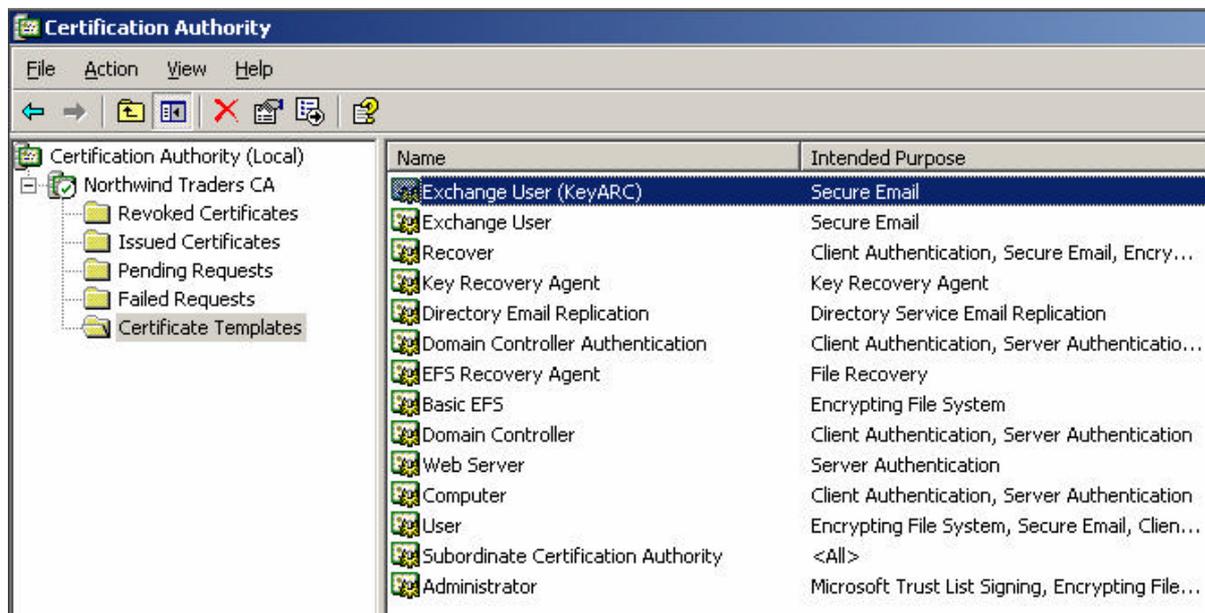


Figure 4: New certificate template

Issue e-mail certificates to users

It is possible to autoenroll user- and machine certificates for all users and computers with Active Directory and Group Policies. Autoenrollment for Users and machines requires a Windows 2003 Active Directory environment and Windows XP clients. For more information about Certificate Autoenrollement, click the link at the end of this article. For this article the user MSEXCHANGEORG will request an *Exchange User (KeyARC)* certificate manually.

Microsoft Certificate Services -- Northwind Traders CA

Advanced Certificate Request

Certificate Template:

Exchange User (KeyARC)

Identifying Information For Offline Template:

Name: MSEXchangeORG

E-Mail: MSEXchangeORG@nwtraders.msft

Company: NWTRADERS

Department: Sales

City: London

State:

Country/Region:

Key Options:

Create new key set Use existing key set

CSP: Microsoft Enhanced Cryptographic Provider v1.0

Key Usage: Exchange

Key Size: 1024 Min: 1024 Max: 16384 (common key sizes: 1024 2048 4096 8192 16384)

Automatic key container name User specified key container name

Mark keys as exportable

Export keys to file

Enable strong private key protection

Store certificate in the local computer certificate store

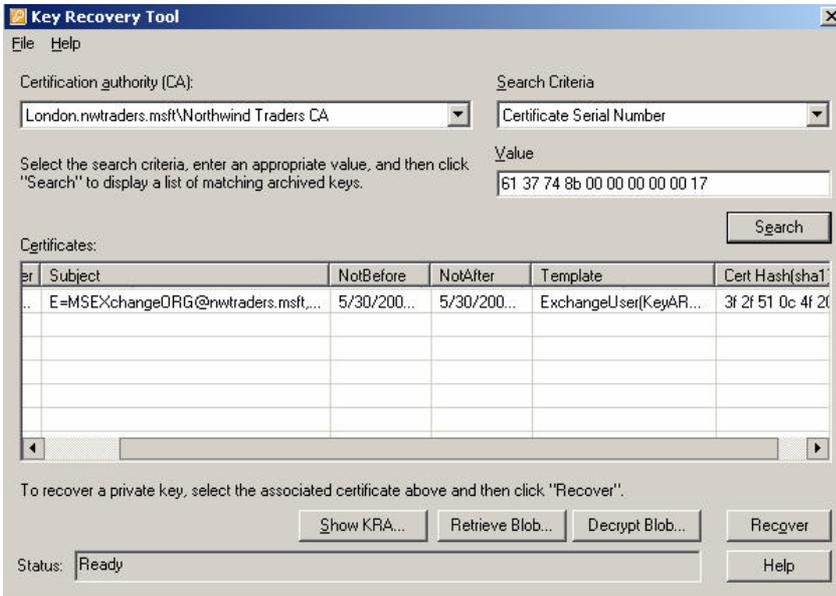


Figure 7: Recovery the users Private Key

You can save the recovered certificate in a file that contains the certificate Serial Number with a PFX extension. I recommend changing the name of the PFX file so it is easier for a user to know what he or she is doubleclicking.

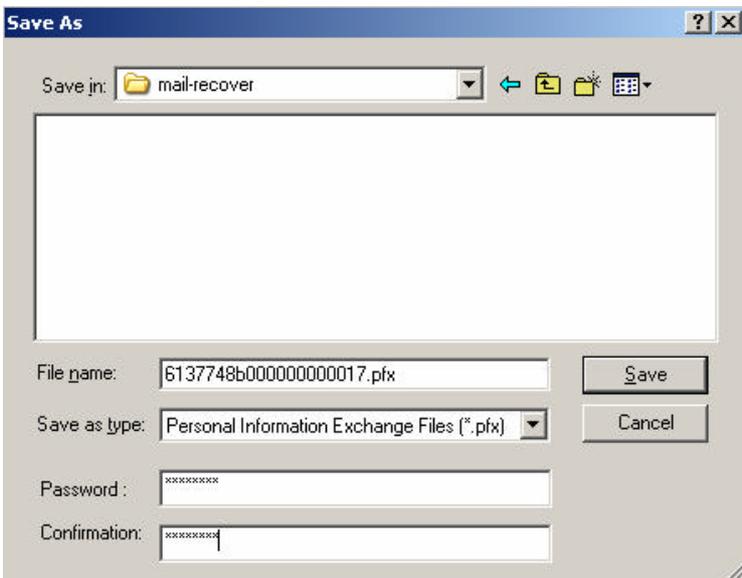


Figure 8: Save the recovered certificate

Now it is time to transmit the certificate to the user. Don't use an E-Mail for delivery because the PFX file contains the private Key for this user. At the user's site, the user can import this certificate by a simple doubleclick.

Conclusion

Key Archiving is a powerful weapon for the Administrator to reduce the time to recovery user's private certificate. At the other hand it is important to secure the CA (Physical and logical) and to give this feature for Key Recovery only to highly trusted Administrators.

Related Links

Certificate Autoenrollment in Windows Server 2003

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/autoenro.mspx>

Managing a Windows Server 2003 Public Key Infrastructure

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/mngpki.mspx>

Exchange 2000 Key Management Server Migration to a Windows 2003 CA

http://www.msexchange.org/tutorials/Key_Management_server_Migration.html

Windows 2003 Resource Kit Tools

<http://www.microsoft.com/downloads/details.aspx?FamilyID=9d467a69-57ff-4ae-96ee-b18c4790cffd&display=en>