Certificate Autoenrollment with Windows .NET Enterprise Server CA and Windows XP Professional as a Client

Written by Marc Grote
MCP, MCP+I, MCSA, MCSE NT4, MCSE Win2K, MCT, CNA, CCNA, CCA
mailto:grotem@it-training-grote.de

Abstract

The Microsoft Windows .NET Server Operating System provides some new enhanced features for deploying a PKI in Windows based operating systems.
This article explains some new features of the Windows .NET Server CA and the autoenrollment of computer certificates for client-authentication with Windows .NET Server Group Policies.
The explanations are based on Windows .NET Server Enterprise Edition – RC2 German and Windows XP Professional with Service Pack I.

Introduction

PKI is short for public key infrastructure. A PKI is a combination of technologies, hardware, software and certificate to secure the modern electronic business with the help of hardware like smartcards and digital certificates to encrypt critical data and to ensure the authentication of business partners.

New PKI features in Windows .NET Server

The new Certificate Authority in Windows .NET Server has a lot of new features. The important features are:

- Central certificate key saving and recovery like the KMS (Key Management Server) in Exchange 2000
- Version 2 certificate templates (ACL for certificate templates, and the possibility to create your own certificate templates based on predefined templates)

The Windows .NET Server Certificate Authority Tool

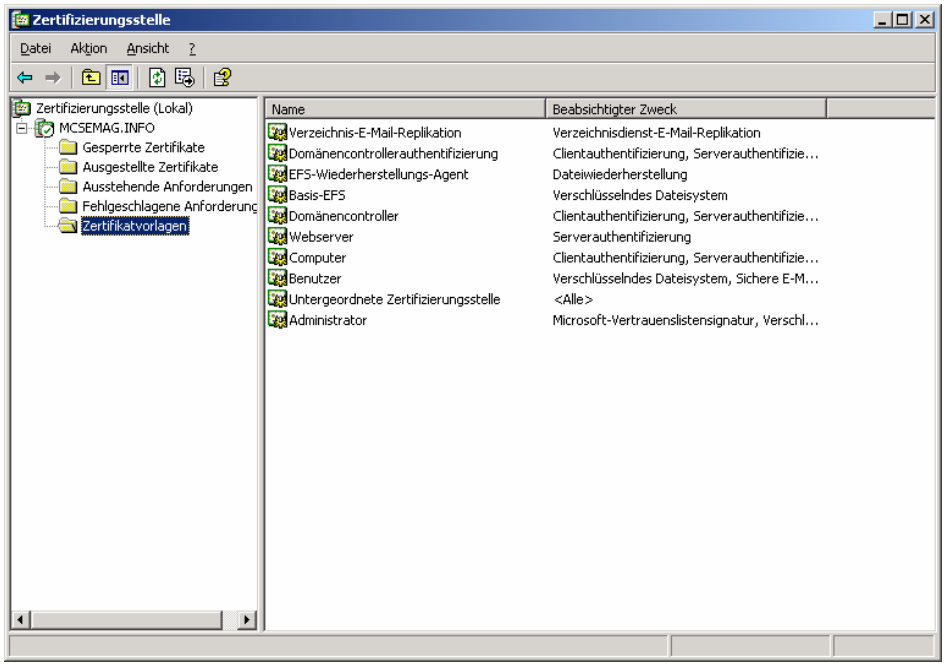

Figure 1: Windows .NET Server Certificate Authority Tool

To deploy certificates for your clients you must use predefined certificate templates or copy a certificate template. Select a required certificate template in the container “certificate template” in the Windows .NET Server Certificate Authority Tool and define the required settings.

Editable Certificate Templates

Certificate templates are used in the Windows .NET Server CA to define templates for special certificate purposes like

- ? E-Mail encryption
- ? Server certificates
- ? IPSEC
  EFS
- ? VPN

Editable certificate templates provide the capability to edit some certificate information like certificate publishing places and ACEs for certificate security. It also includes changes to meet the X.509 standard to include deployment specific information in the certificates and certificate templates.

Windows .NET Server supports two types of certificate templates:

- ? Certificate templates version 1 primary used in Windows 2000 and
- ? Certificate templates version 2 primary used in Windows .NET Server.

Version 1 templates are only readable, predefined templates provided by Microsoft for Windows 2000
Version 2 templates are editable templates from Microsoft for Windows .NET Server. Only Windows .NET Server supports version 2 certificate templates

The ACL and their ACEs in version 2 certificate templates define the security rights to enroll and use certificates.

A user or computer must have both enroll and read permissions to enroll a selected certificate template.
The read permission for the certificate template is necessary to enumerate the templates for the user.
The enroll permission is enforced by the enterprise CA when the user requests a certificate for a template.
The enterprise certification authority must also have read permissions on a template in order to enumerate the template in the directory and issue certificates based on that template. The enterprise certificate authority is included in the Authenticated Users group which has read permissions by default on a template.

The Full Control permission is given to enterprise administrators and the primary domain administrators group by default when installing a fresh Windows .NET domain.

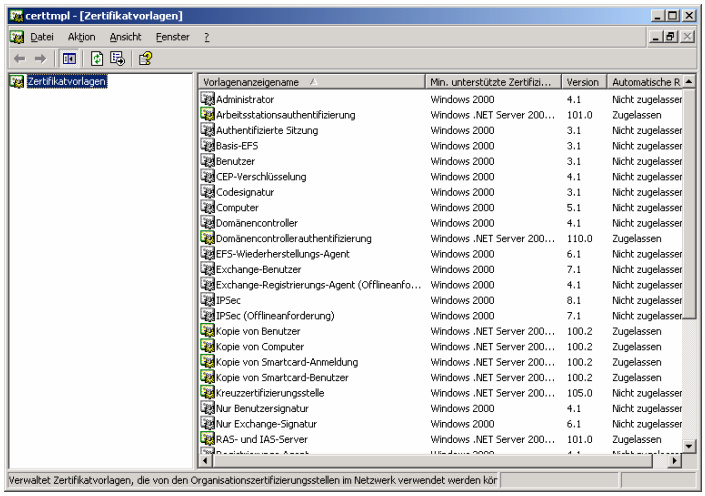

Figure 2: Windows .NET Server Certificate Template Tool

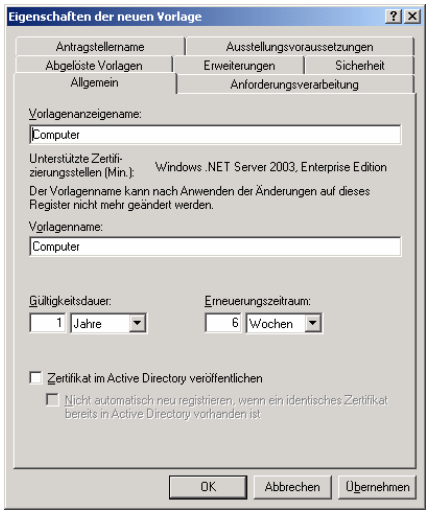

Figure 3: Certificate Template details

Configure a Group Policy for autoenrollment of computer certificates

The next step is to configure an appropriate group policy for certificate autoenrollment. Select an organizational unit and create a new group policy. Under Computer-Configuration – Windows Settings – Public Key Policies – select the required settings and publish the certificates in the console.

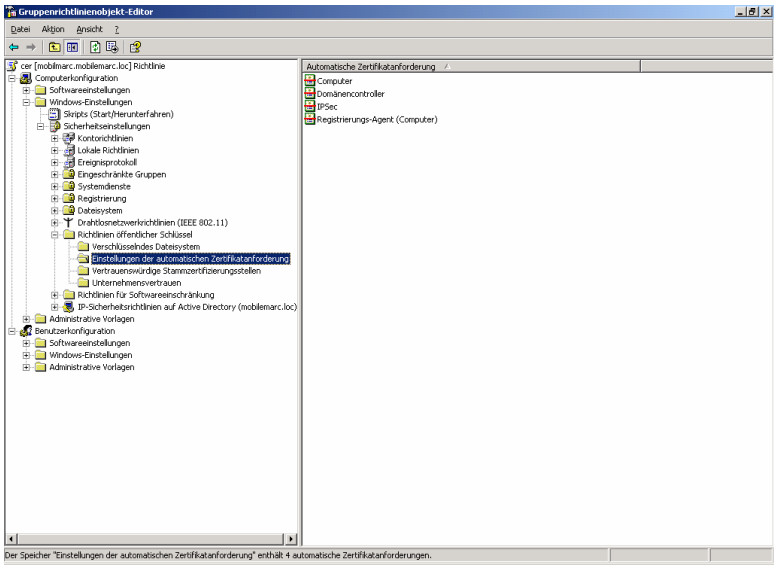

Figure 4: Windows .NET Server Group Policy

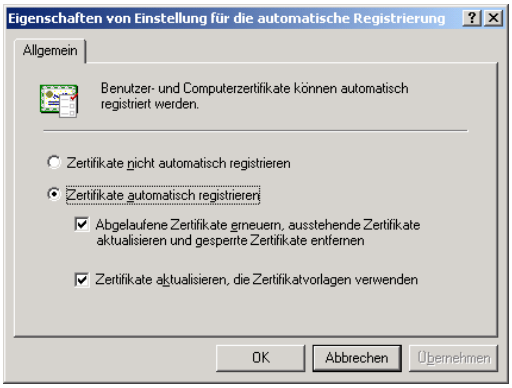

Figure 5: Certificate autoenrollment settings

Certificate autoenrollment

Certificate autoenrollment is based on the combination of group policy settings and version 2 certificate templates. This combination allows Windows XP Professional to enroll certificates to clients when the machine boots or to users when they log on to the domain. Autoenrollment minimizes the cost for PKI deployments because no user interaction is required when the Windows XP Clients are members of a Windows 2000 / Windows .NET Server Domain.

The autoenrollment feature in Windows .NET Server has several requirements. These include:

- Windows .NET domain controllers
- Windows XP Client
- Windows .NET Enterprise Edition running as an Enterprise certificate authority (CA)

The certificate autoenrollment is based on the winlogon process. For computer policies the policies are applied at computer startup. Policies for users are applied at logon (after Winlogon starts).

Once a certificate template has been enumerated through the selected group policy the autoenrollment process will search for a CA in Active Directory through LDAP. The first responding CA – if multiple CAs are available - will issue a certificate through the client or user logon process.

Renewing a Certificate

The certificate renewing process of an expired user or computer certificate can also take advantage of the autoenrollment mechanism. Certificates are automatically renewed when the defined lifetime on the certificate expires.

Conclusion

The technique to autoenroll certificates in combination with Active Directory and Group Policies reduce the implementation- and administration cost in a Microsoft PKI environment in an important way and is a significant step to reduce the TCO (Total Cost of Ownership) in a Microsoft Windows network environment.

Related Links (Based on the Microsoft Whitepaper CertifAutoEnroll.doc)

Windows 2000 Security Services at http://www.microsoft.com/windows2000/technologies/security/default.asp
What's New in Security for Windows XP Professional and Windows XP Home Edition at http://www.microsoft.com/windowsxp/pro/techinfo/planning/security/whatsnew/default.asp
Windows XP and .NET: An Overview at http://www.microsoft.com/windowsxp/pro/techinfo/planning/dotnet/default.asp
Data Protection and Recovery in Windows XP at http://www.microsoft.com/windowsxp/pro/techinfo/administration/recovery/default.asp
Securing Mobile Computers with Windows XP Professional at http://www.microsoft.com/windowsxp/pro/techinfo/administration/mobile/default.asp
PKI Enhancements in Windows XP Professional and Windows .NET Server at http://www.microsoft.com/windowsxp/pro/techinfo/planning/pkiwinxp/default.asp