



# Active Directory Certificate Server Enhancements in Windows Server “Longhorn”

Microsoft Corporation

Published: September 2006

Authors: Carsten B. Kinder

Contributors: Avi Ben Menahem, Oded Shekel

Abstract

Microsoft® Active Directory® Certificate Services in the Microsoft Windows Vista™ and Windows Server® "Longhorn" operating systems provides an infrastructure for improved X.509 certificate management. Expanding on the foundation established in the Microsoft Windows Server 2003 and Microsoft Windows® XP operating systems, Active Directory Certificate Services has been improved with greater manageability, smoother Windows integration, and is also more compliant with standards. This guide provides an overview of new features and improvements in Active Directory Certificate Services.



Disclaimer

This document supports a preliminary release of a software product that may be changed substantially prior to final commercial release. The document was written based on Beta 2 of Windows Server “Longhorn”. This document is provided for informational purposes only and Microsoft makes no warranties, either express or implied, in this document. Information in this document, including URL and other Internet Web site references, is subject to change without notice. The entire risk of the use or the results from the use of this document remains with the user. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2006 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, BitLocker, Outlook, Windows, Windows logo, Windows Server, Windows Server System, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.

Contents

[Active Directory Certificate Server Enhancements in Windows Server “Longhorn” 1](#_Toc147197076)

[Overview 7](#_Toc147197077)

[About This Document 7](#_Toc147197078)

[Scope 7](#_Toc147197079)

[Related Information 7](#_Toc147197080)

[Introduction 7](#_Toc147197081)

[Deployment and Configuration 8](#_Toc147197082)

[Advanced Cryptography Support 9](#_Toc147197083)

[Cryptography API: Next Generation 9](#_Toc147197084)

[Support for Discrete Signatures 13](#_Toc147197085)

[Interactive Setup 14](#_Toc147197086)

[Overview and Requirements 14](#_Toc147197087)

[Scenario 16](#_Toc147197088)

[Configuration 18](#_Toc147197089)

[Setup Permissions to Install Certificate Services 21](#_Toc147197090)

[Working with the Add Roles Wizard 21](#_Toc147197091)

[Setting Up the Active Directory Certificate Server Role with the CA Role Service 23](#_Toc147197092)

[Adding a Role Service 31](#_Toc147197093)

[Removing Active Directory Certificate Services as a Server Role 32](#_Toc147197094)

[Removing Role Services from Active Directory Certificate Services 33](#_Toc147197095)

[Role Service Default Settings 33](#_Toc147197096)

[Configuring Active Directory Certificate Services Using a CAPolicy.inf File 34](#_Toc147197097)

[CDP and AIA Certificate Attributes 35](#_Toc147197098)

[Avoiding an Immediate Load of Default Certificate Templates During Setup 35](#_Toc147197099)

[Using Discrete Signatures for the CA Certificates or CA Certificate Requests 36](#_Toc147197100)

[Using Discrete Signatures for Issued Certificates 36](#_Toc147197101)

[Troubleshooting 37](#_Toc147197102)

[Active Directory Certificate Services service terminated with service-specific error 2148081683 (0x80092013) 37](#_Toc147197103)

[Web enrollment support cannot be installed on a different machine than the Certification Authority 37](#_Toc147197104)

[Upgrade 38](#_Toc147197105)

[Overview and Requirements 38](#_Toc147197106)

[Scenario 38](#_Toc147197107)

[Configuration 39](#_Toc147197108)

[Troubleshooting 39](#_Toc147197109)

[Configuring the Cryptographic Algorithms used by the CA 39](#_Toc147197110)

[Configuration 39](#_Toc147197111)

[Certificate Templates 43](#_Toc147197112)

[Overview and Requirements 43](#_Toc147197113)

[Scenario 44](#_Toc147197114)

[Configuration 45](#_Toc147197115)

[Upgrading the Default Templates 45](#_Toc147197116)

[Connecting the Certificate Templates MMC Snap-In to a Specific Domain Controller 46](#_Toc147197117)

[Creating V3 Certificate Templates 46](#_Toc147197118)

[Customizing Windows Vista Certificate Templates 47](#_Toc147197119)

[Default Certificate Templates in Windows Server 2003 and Windows Server “Longhorn” 48](#_Toc147197120)

[Troubleshooting 49](#_Toc147197121)

[certutil -template output is incomplete 49](#_Toc147197122)

[certificate templates are not available 49](#_Toc147197123)

[Restricted Enrollment Agent 50](#_Toc147197124)

[Overview and Requirements 50](#_Toc147197125)

[Scenario 51](#_Toc147197126)

[Configuration 52](#_Toc147197127)

[Troubleshooting 55](#_Toc147197128)

[Certificate templates do not appear in the Add certificate template dialog 55](#_Toc147197129)

[“No properties are available on this object.” when opening a V3 certificate template 55](#_Toc147197130)

[Restricted Certificate Managers 55](#_Toc147197131)

[Overview and Requirements 55](#_Toc147197132)

[Scenario 55](#_Toc147197133)

[Configuration 56](#_Toc147197134)

[Troubleshooting 59](#_Toc147197135)

[The Certification Authorities properties dialog does not match the screenshots from above 60](#_Toc147197136)

[You cannot add or remove certificate managers from the “Certificate Managers” dialog 60](#_Toc147197137)

[A SID appears in the Certificate Managers or Permissions list box instead of the user or group name 60](#_Toc147197138)

[Key Archival and Recovery 60](#_Toc147197139)

[Overview and Requirements 60](#_Toc147197140)

[Scenario 61](#_Toc147197141)

[Configuration 61](#_Toc147197142)

[Performing Key Recovery at the Command Line 61](#_Toc147197143)

[Changing Cryptographic Algorithms for Key Exchange and Key Archival 62](#_Toc147197144)

[Performance Counters 68](#_Toc147197145)

[Overview and Requirements 68](#_Toc147197146)

[Scenario 69](#_Toc147197147)

[Monitoring During Initial Certificate Enrollment 69](#_Toc147197148)

[Collecting Data to Create Health Reports to Back Up Service Level Agreements 70](#_Toc147197149)

[Configuration 70](#_Toc147197150)

[Troubleshooting 71](#_Toc147197151)

[Performance Counters are not installed properly after re-installation of Certificate Service 71](#_Toc147197152)

[Manual Certificate Enrollment 72](#_Toc147197153)

[Configuring Support for the Discrete Signature Algorithm (PKCS#1 V2.1 signatures) for CNG 72](#_Toc147197154)

[Windows Integration 73](#_Toc147197155)

[Enterprise PKI (PKIview) 74](#_Toc147197156)

[Overview and Requirements 74](#_Toc147197157)

[Scenario 74](#_Toc147197158)

[Configuration 74](#_Toc147197159)

[Troubleshooting 77](#_Toc147197160)

[Enabling CAPI2 logging to troubleshoot chain validation errors 78](#_Toc147197161)

[Web Enrollment 79](#_Toc147197162)

[Overview and Requirements 80](#_Toc147197163)

[Scenario 80](#_Toc147197164)

[Configuration 81](#_Toc147197165)

[Installing Multiple Languages for Certificate Web Enrollment on a Single Server 81](#_Toc147197166)

[Upgrading Web Enrollment Support from Windows Server 2003 to Windows Server Longhorn 83](#_Toc147197167)

[Installation of 64-Bit Web Enrollment on an IIS Computer that Runs 32-Bit Web Applications 83](#_Toc147197168)

[Troubleshooting 84](#_Toc147197169)

[Server Error in 'Default Web Site/CertSrv' Application.*HTTP Error 404.0 - Not Found* 84](#_Toc147197170)

[The Web site cannot display the page 84](#_Toc147197171)

[Removing the Certification Authority from a computer where Web enrollment is installed fails 84](#_Toc147197172)

[KDC Certificate Modification 85](#_Toc147197173)

[Overview and Requirements 85](#_Toc147197174)

[Scenario 86](#_Toc147197175)

[Configuration 86](#_Toc147197176)

[Differences in Domain Controller Certificate Templates 87](#_Toc147197177)

[Configuring Domain Controller Certificate Templates in Mixed Environments 87](#_Toc147197178)

[Compliant with Standards 89](#_Toc147197179)

[IDP CRL Extension Support 89](#_Toc147197180)

[Overview and Requirements 89](#_Toc147197181)

[Scenario 90](#_Toc147197182)

[Configuration 90](#_Toc147197183)

[OCSP Support 91](#_Toc147197184)

[MSCEP 92](#_Toc147197185)

# Overview

## About This Document

Active Directory Certificate Services introduces enhancements to several functional areas in the Windows Server “Longhorn” release. Most of the features detailed in this document are the result of customer requirements for an improved feature set from the Certificate Server.

This document does not cover functionality that already exists in the Windows Server 2003 release of the Certificate Services.

## Scope

This document provides an overview of the new features that are implemented in the Windows Server “Longhorn” release of the Active Directory Certificate Server. It is not an introduction to public key infrastructure (PKI) technologies, Certification Authorities (CAs), or certificates. It assumes that the reader has a good understanding of PKI and Active Directory concepts.

The document does not cover the Certificate Lifecycle Management product, which is a separate product.

## Related Information

For general documentation about the Windows PKI, see
<http://www.microsoft.com/pki>

For more information about Certificate Lifecycle Management, see
<http://www.microsoft.com/clm>

## Introduction

The investment that was made in Active Directory Certificate Services can be divided into three main areas.

* Deployment and Configuration
* Windows Integration
* Compliant with Standards

The following chapters cover all improvements that have been made in these specific areas and their subcategories.

Windows Server “Longhorn” offers a Standard Edition and an Enterprise Edition Certification Authority. The following table lists the new features based on the CA type.

|  |  |  |
| --- | --- | --- |
| **Feature** | **Standard Edition** | **Enterprise Edition** |
|  | Windows integration |
| Advanced cryptography support | Available | Available |
| Failover cluster support | Requires at least Windows Server “Longhorn” Beta 3 | Requires at least Windows Server “Longhorn” Beta 3 |
| Enterprise PKI (PKIview) | Available(content depends on PKI configuration) | Available(content depends on PKI configuration) |
| Web enrollment | Available | Available |
| KDC certificate modification | Not available | Available |
| Deployment and Configuration |
| Setup with the Role Management tool | Available | Available |
| Upgrade | From previous Standard Certification Authority | From previous Standard or Enterprise Certification Authority |
| Unattended setup | Available | Available |
| V3 certificate templates | Not available | Available |
| Restricted enrollment agent | Not available | Available |
| Restricted certificate managers | Not available | Available |
| Key archival enhancements | Not available | Available |
| Performance counters | Available | Available |
| Compliant with Standards |
| IDP CRL extension support | Available | Available |
| SCEP | Not available | Available |
| OCSP | Not available | Available |

# Deployment and Configuration

This section discusses the following improvements to the Windows Server “Longhorn” Active Directory Certificate Services, which benefit the Certificate Services administrator.

* Advanced Cryptography Support for new cryptographic algorithms and discrete signatures.
* Setup of certificate services and its related role services such as Web enrollment.
* Upgrade from a previous Windows version of Certificate Services.
* Unattended setup to install a Certificate Service or role service without user interaction.
* Certificate templates to define new certificate characteristics.
* Restricted enrollment agent to control who is able to enroll certificates on behalf of a specific user or group.
* Restricted certificate managers to control who may approve or revoke certificates for a specific user or group.
* Key archival to protect private keys with stronger encryption algorithms.
* Performance counters to monitor the performance and health of certificate services.

## Advanced Cryptography Support

The Advanced Cryptography Support is a new infrastructure component in Windows and is also used by Active Directory Certificate Services. Because Cryptography API: Next Generation (CNG) is relevant in several sections of this document, this section provides an overview, and details are provided in each section where CNG applies.

### Cryptography API: Next Generation

Microsoft introduces a completely new cryptography API in Windows Vista and “Longhorn” Server. CNG API is the long-term replacement for the CryptoAPI. CNG implements the Suite-B protocols so that both terms are interchangeable in this document.

One of the CNG features is the ability for customers to use their own cryptographic algorithms or implementations of standard cryptographic algorithms if desired. This also covers the ability to add new algorithms as required. A CA installed on a Windows Server 2003 computer supports only cryptographic algorithms such as RSA or SHA1 through cryptographic service providers (CSPs). With Windows Vista and Windows Server “Longhorn”, classic cryptographic algorithms are still supported through CSPs, but also new algorithms like Elliptic Curve Cryptography (ECC) are supported through CNG key providers. Figure 1 illustrates the overall CNG architecture.



Figure : CNG Architecture

For more information about CNG, see
<http://msdn.microsoft.com/library/en-us/seccng/security/cng_portal.asp>

CNG is not only relevant for developers who might use this new platform technology to support other cryptographic algorithms in their applications, but it also changes the requirements of the underlying PKI.

Currently, CNG–based algorithms such as ECC are only supported on Windows Vista and Windows Server “Longhorn”. This means that those certificates cannot be used on earlier Windows versions such as Windows XP or Windows Server 2003. However, classic algorithms such as RSA can be used even if the keys have been generated with a CNG key provider.

To use the new cryptographic algorithms, both your CA and your applications should support ECC. While the CA needs to issue and manage these new certificate types, applications must be able to handle certificate chain validation and use the keys generated with CNG algorithms.



Important

Before issuing certificates that use Suite-B algorithms like ECC, you have to make sure that your CA and the operating systems that have to handle these certificates support these algorithms.

At the same time, you have to evaluate if the PKI–enabled applications are ready to deal with certificates that use Suite-B cryptographic.

In case of smart card logon, you have to verify with your smart card vendor that the smart cards are able to handle Suite-B algorithms.

You should not deploy certificates with Suite-B cryptographic before these requirements are satisfied.

In Windows Vista and Windows Server “Longhorn”, the following certificate-enabled applications are able to handle certificates that use Suite-B algorithms.

|  |  |  |
| --- | --- | --- |
| Application Name | Verify a certificate chain that contains certificates with Suite-B algorithms.  | Use algorithms that are not supported by CAPI (CSP). |
| EFS | Yes | No |
| IPsec | Yes | Yes |
| Kerberos | No | No |
| S/MIME | Microsoft Outlook® 2003: noOutlook 2007: yes | Outlook 2003: noOutlook 2007: yes |
| Smart Card Logon | No (in the beta 2 release) | No (in the beta 2 release) |
| SSL | Yes | Yes |
| Wireless | Yes | Yes |

This document mentions CNG in multiple sections because the use of CNG can be configured at various places.

* To configure CNG for the CA signing certificate, see "Configuring the Cryptographic Algorithms used by the CA".
* To configure CNG for the CA key exchange certificate, see "Changing the Key Archival Algorithm for the CA".
* To configure CNG for the key archival encryption algorithm, see "Changing the Key Archival Algorithm for the CA".
* To configure CNG with certificate templates, see "Customizing Windows Vista Certificate Templates".
* To use CNG algorithms for manual certificate requests, see "Configuring Support for the Discrete Signature Algorithm (PKCS#1 V2.1 signatures) for CNG".

If you want to use the new algorithms and their configuration options, it is required to plan well in advance before you migrating from the “classic” algorithms to the new Suite-B algorithms.

To actually use Suite-B algorithms for cryptographic operations, you first need a Windows Server “Longhorn” CA to issue certificates with Suite-B algorithms.

If you do not yet have a PKI, you may consider setting up one where the CA certificates and the end-entity certificates use Suite-B algorithms. However, first ensure that all your applications are ready for Suite-B and will support such certificates. For information about setting up the root CA and subordinate CAs with Suite-B algorithms, see "Interactive Setup".

If you have a PKI already where classic algorithms are in place, you can add Windows Server “Longhorn” computers as subordinate CAs and also use the classic algorithms. Configuring a add Windows Server “Longhorn” as a subordinate CA with Suite-B algorithms might not be very useful because you cannot change the algorithms that are used by its parent CAs. To introduce Suite-B into an existing environment where classic algorithms are used, consider a second CA hierarchy and perform a cross-certification between the existing hierarchy and the new hierarchy as illustrated in Figure 2.



Figure : Extending a PKI with CNG Algorithms

### Support for Discrete Signatures

With the introduction of new signature and encryption algorithms, it was necessary to include additional information in a certificate or a certificate request about which algorithm was used to generate a signature. Without having this information in a certificate or certificate request, it is not possible for an entity that processes the certificate or certificate request to verify the signature of a certificate or a request.

Generally, to create a signature, a hash needs to be generated with binary data such as a certificate or a certificate request. A hashing algorithm like SHA1 or MD5 is used to do this. Once the hash is calculated, it is signed with an asymmetric key like RSA or Elliptic Curve Digital Signature Algorithm (ECDSA) as illustrated in Figure 3.



Figure : A hashed Certificate Request with a Signature

With an increasing number of available algorithms, the number of possible combinations for hash and signature algorithms is growing. For example, a certificate request might be hashed with a SHA1 and signed with RSA but the issued certificate was hashed with SHA512 and signed with ECDSA\_P384. Therefore, it is required to add information about the used algorithms into the certificate or request instead of maintaining a list of identifiers that translate the combinations. Discrete signatures for RSA–based certificates are documented as part of the PKCS #1: RSA Cryptography Standard. For more information about the standard, see the RSA Web site at
<http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/>

Windows Vista and Windows Server “Longhorn” support discrete signatures in various scenarios. The configuration of discrete signatures is described in several sections in this document.

There are various areas where discrete signatures can be configured. The following summarizes in which areas discrete signatures for certificates or certificate requests can be enabled.

* To create a root CA certificate with a discrete signature, you have to set the DiscreteSignatureAlgorithm parameter in the capolicy.inf file of the root CA before setting it up or before renewing the root CA certificate. For more information, see "Using Discrete Signatures for the CA Certificates or CA Certificate Requests".
* To create a certificate request for a subordinate CA certificate that carries a discrete signature, you have to set the DiscreteSignatureAlgorithm parameter in the capolicy.inf file of the subordinate CA before setting it up or before renewing the root CA certificate. For more information, see "Using Discrete Signatures for the CA Certificates or CA Certificate Requests".
* For Windows clients that use auto enrollment or the Certificates Microsoft Management Console (MMC) Snap-In to generate certificate requests that carry a discrete signature, you have to select the "Discrete Signature" option in the certificate template that is used to enroll the certificate. For more information, see "Customizing Windows Vista Certificate Templates".
* To create a certificate request manually with certreq.exe, you have to set the DiscreteSignatureAlgorithm parameter in the .inf file that is used to create the certificate request. For more information, see "Configuring Support for the Discrete Signature Algorithm (PKCS#1 V2.1 signatures) for CNG".
* To issue certificates that carry a discrete signature, you have to set the DiscreteSignatureAlgorithm registry key at the CA that issues certificates. This can either be a root CA or a subordinate CA. For more information, see "Using Discrete Signatures for Issued Certificates".

## Interactive Setup

This section describes the changes that have been made to set up a new CA.

### Overview and Requirements

One of the design goals of the add Windows Server “Longhorn” release is to make Windows a componentized operating system. Therefore, a lot of engineering effort has been invested to redesign the management of Windows Server components.

Active Directory Certificate Services setup is done through the Server Manager Tool—a wizard-based tool that was designed to improve the user experience in setting up optional components to Windows Server. The improvements include:

* Improved usability.
* Fewer steps for installation and more predefined defaults.
* Improved errors and warning.
* Unattended setup.

In addition to improving the setup experience, Windows Server includes a one place tool for monitoring Optional Components that are installed.

The Server Manager differentiates mainly between server features, server and role services.

* Server Feature. An optional core function of Windows Server Longhorn, such as BitLocker™, Failover Clustering, or Microsoft Message Queuing (MSMQ). It is usually used by more than one application, role, or role feature.
* Server Role. A primary set of functions that a server can perform, such as file/print server, domain controller, and certificate server. It can use numerous features and can also include role services. It is not a piece of software, but is a logical definition. A role is always represented by one or many role services.
* Role Service. For example, the CA or Online Certificate Status Protocol (OCSP) represents a server.

Server Manager supports installation of multiple roles or role services as a one step experience unless there are dependencies between the roles or services.

Certificate Server in Windows Server “Longhorn” consists of the following four role services.

* Certification Authority
* Certification Authority Web Enrollment
* Online Certificate Status Protocol
* Microsoft Simple Certificate Enrollment Protocol

Server features are not relevant for Certificate Services, therefore, they are not discussed further in this section.

To install the Certification Authority Web Enrollment (CAWE), the OCSP, or the Microsoft Simple Certificate Enrollment Protocol (MSCEP), you must have the Internet Information Services (IIS) role services installed on the system as shown in the following table. The Roles Management Tool (RMT) takes care of all internal component dependencies and installs missing components automatically.

|  |  |  |  |
| --- | --- | --- | --- |
|  | CAWE | OCSP | MSCEP |
| Web Server (IIS) |  |  |  |
|  Web Server |  |  |  |
|  Common HTTP Features |  |  |  |
|  Static Content | 🗹 | 🗹 | 🗹 |
|  Default Document | 🗹 | 🗹 | 🗹 |
|  Directory Browse | 🗹 | 🗹 | 🗹 |
|  HTTP Errors | 🗹 | 🗹 | 🗹 |
|  HTTP Redirection | 🗹 | 🗹 | 🗹 |
|  Performance |  |  |  |
|  Static Content Compression | 🗹 | 🗹 | 🗹 |
|  Health and Diagnostics |  |  |  |
|  HTTP Logging | 🗹 | 🗹 | 🗹 |
|  Logging Tools | 🗹 | 🗹 | 🗹 |
|  Request Monitor | 🗹 | 🗹 | 🗹 |
|  Tracing | 🗹 | 🗹 | 🗹 |
|  Application Development |  |  |  |
|  .NET Extensibility | 🗹 | 🗹 | 🗹 |
|  ASP | 🗹 | 🗷 | 🗷 |
|  ISAPI Extensions | 🗹 | 🗹 | 🗹 |
|  Security |  |  |  |
|  Request Filtering | 🗹 | 🗹 | 🗹 |
|  Windows Authentication | 🗹 | 🗷 | 🗹 |
|  Web Server Management Tools |  |  |  |
|  IIS Management Console | 🗹 | 🗹 | 🗹 |
|  IIS 6 Management Compatibility |  |  |  |
|  IIS MetaBase Compatibility | 🗹 | 🗹 | 🗹 |
| Windows Activation Service (WAS) |  |  |  |
|  Process Model | 🗹 | 🗹 | 🗹 |
|  .NET Environment | 🗹 | 🗹 | 🗹 |
|  Configuration APIs | 🗹 | 🗹 | 🗹 |

As you can see in the table, OCSP does not require Windows Authentication and Active Server Pages (ASP) while MSCEP does not require ASP. All other Web Server components are similar amongst all three role services.

### Scenario

Installing the Active Directory Certificate Server role allows multiple choices regarding the topology and service distribution.

Technically, there is a choice between installing particular or all-role services on a single server or distributing the role services across multiple servers. Also, there is a choice between installing Active Directory Certificate Server in an Active Directory environment or using stand-alone servers.

Generally, an Active Directory environment is recommended for issuing CAs. The root CA should be on a stand-alone system that is not member of an Active Directory environment and not connected to any network.

The number of servers and the level of service distribution depend on your requirements regarding security and availability. Figure 4 illustrates common options for how a PKI can be implemented.



Figure : Security and Availability Requirements

* If you have only a single server available to deploy your PKI, you should install the role services CA and, if required, CAWE on that server. Assuming that single server deployments are more common in small and medium businesses, it is unlikely that you require OCSP and MSCEP support. If you still require OCSP and MSCEP, install those role services also on this server. Remember that this is the less secure solution with the lowest availability.
* If you can afford three servers to deploy your PKI, you might install a CA role service as root CA on the first server and install the issuing CA role service on the second server. If required, install the CAWE, OCSP, and MSCEP also on the third server. This PKI can be extended with more servers to increase the availability.
* If you require a high secure and highly available PKI, you should invest in six or more physical servers. Host-based or network hardware security modules (HSM) should be part of a high security PKI, and secure the private keys of at least the root CA. The role services for the root CA are installed on the first server. The issuing CAs are installed on the second and third server. The OCSP responder would be on the fourth and fifth server where both servers form an IIS cluster. The sixth server can handle the role services for CA Web-enrollment and MSCEP if these services are required. For more information about how to set up a highly secure and highly available PKI, see the “Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure” document at
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws3pkibp.mspx

### Configuration

Windows Server “Longhorn” introduces a completely new concept of software installation and configuration. In previous Windows versions, Windows components are installed through the Optional Component Manager in the Windows control panel. This framework is replaced in Windows Server “Longhorn” with the RMT represented through the Server Manager MMC Snap-In.

To set up a new CA, use one of the following applications.

* Initial Configuration Tasks
* Server Manager

The **Initial Configuration Tasks** dialog box appears after a user with local administrator permissions logs on to a Windows Server “Longhorn” for the first time (Figure 5).



Figure : Initial Configuration Tasks

Use the **Initial Configuration Tasks** dialog box to perform the most important configuration tasks right after a server installation from a central location. A CA can be added to a Windows Server “Longhorn” through the **Add roles** option in the **Customize this server** section.

Unless the **Do not show this window at logon** check box is selected, the **Initial Configuration Tasks** dialog box re-appears every time the user logs on to the Windows Server Longhorn.

If the **Initial Configuration Tasks** dialog box does not appear again after logging on to a Windows Server Longhorn, Active Directory Certificate Server is to be installed with the Server Manager MMC Snap-In. This MMC Snap-In provides an **Add roles** option in the **Manage Roles** section (Figure 6).



Figure : Server Manager

Regardless of whether the Initial Configuration Tasks dialog box or the Server Manager MMC Snap-In is used to add the Active Directory Certificate Server role, the Setup wizard is the same in both cases.

Before launching the wizard to install a CA, you should have planned for a number of configuration parameters. You will need to decide the following:

* If the CA is an Active Directory–integrated enterprise CA or a stand-alone CA.
* If the CA is a root CA or a subordinate CA.
* If you want the CA to generate a new private key or if an existing private key is used. For a new private key, you also have to plan for the cryptography configuration.
* Which cryptographic provider should be used to generate the new key?
* What is the key-character length?
* What hash algorithm is used to sign certificates issued by this CA?
* If provided, should strong private key protection be used? Usually HSMs provide an additional authentication mechanism to protect the private key of the CA.
* What will be the common name for this CA?
* How is the distinguished name suffix defined?
* How long will the certificates of this CA be valid?
* What will be the name of the CA? The computer name and the domain name will become part of the subject name of an enterprise CA and cannot be changed at a later stage.
* Where will the certificate database be located on the file system?
* Where will the certificate database log be located on the file system?



Note

Certificate services in Windows Server “Longhorn” support new CSPs that are capable of dealing with advanced hash algorithms like SHA2. Choosing such a new algorithm type requires careful planning and a good migration strategy if you already have a PKI in place.

If you have followed the setup or removal process outlined in the following sections, you can verify the state and configuration of the Active Directory Certificate Server role also in Server Manager. Figure 7 shows an example of the Role Management window.



Figure : Role Management Window

This window in Server Manager is also helpful during normal operations to quickly access the role-specific administration tasks.

#### Setup Permissions to Install Certificate Services

Depending on the scenario and environment, different permissions are required to install different role services. The following list shows the permissions that are required for each individual role.

* Enterprise Certification Authority: Enterprise Administrator.
* Stand-alone Certification Authority in a workgroup computer: local Administrator.
* Stand-alone Certification Authority on a domain-joined computer: Certification Authority certificate and Certificate Revocation List (CRL) are not published in the Active Directory configuration container if non-Enterprise Administrator is installing the role.
* Certification Authority Web Enrollment: local Administrator.
* Online Certificate Status Protocol: local Administrator.
* Microsoft Simple Certificate Enrollment Protocol targeted to a stand-alone Certification Authority: local Administrator.
* Microsoft Simple Certificate Enrollment Protocol targeted to an Enterprise Certification Authority: local Administrator and Enterprise Administrator to assign templates to the CA and modify the access control list (ACL) on templates.

#### Working with the Add Roles Wizard

The Add Roles Wizard is not specific to certificate services. It provides a unique interface to install server roles generally on a Windows Server Longhorn.

To install a multi-purpose server, several roles can be installed at a time. In this case, the configuration dialog boxes for each role are added to the list of installation options.

Figure 8 illustrates the Add Roles Wizard to install all role services for certificate services.



Figure : Add Roles Wizard

The left side of the window lists all configuration options that are available to install the services that have been selected in the center of the window. To maneuver directly to a specific installation option, click the enabled, black-colored items. Disabled, grey-colored items indicate that an enabled configuration option must be completed before the disabled option becomes available.

The Install button stays disabled until all required configuration options are provided with a configuration parameter. Most of the options have default values but some require explicit configuration. If you have chosen the MSCEP role service, you must have accessed the **Replace RA Certificates** configuration option and **Specify User Account** before the **Install** button becomes enabled.

Once the Install button becomes enabled, the installation of all selected role services can be performed.

**Note** Even if most configuration options have default values, it is highly recommended to explicitly configure the settings for Certificate Services. A CA is a long-run infrastructure component that requires good planning and configuration.

#### Setting Up the Active Directory Certificate Server Role with the CA Role Service

The following steps describe how an Active Directory Certificate Server role is added on the Server Manager MMC Snap-In. Remember that any of the four service roles (Certification Authority, Certification Authority Web Enrollment, Online Certificate Status Protocol, or Microsoft Simple Certificate Enrollment Protocol) can represent the Active Directory Certificate Server role.

If you recognize that you have made a configuration error in the wizard, instead of clicking the **Previous** button multiple times, click the name of the task in the left pane of the wizard and go directly to the dialog box where the configuration change is required.

In this example, an enterprise subordinate CA is set up, which assumes that you have a root CA already in place. The root CA can be any CA that is able to issue an X.509 CA certificate.

1. Log on to the Windows Server “Longhorn” with Enterprise Administrator permissions.
2. If you are re-installing a CA, make sure that the %SYSTEMROOT%\system32\CertLog directory does not exist or is empty. The Installation wizard in Windows Server “Longhorn” Beta 2 will override an existing database without notifying you. This issue will be resolved in a future preliminary version of Windows Server Longhorn.
3. On the Start menu, select Administrative Tools, and then select Server Manager. Server Manager can also be launched from a command-line prompt using **ServerManager.msc**.
4. In the Server Manager MMC Snap-In, select the Manage Roles node in the left pane.
5. In the right pane, select Add roles in the Roles Summary section.
6. If the Before You Begin window appears, click Next.
7. In the Select Server Roles window, select the Active Directory Certificate Server check box, and then click Next.
8. After reading the Introduction to Active Directory Certificate Services, click Next.
9. Select the Certification Authority role services, and then click Next. Technically, you can select any other role service and start from there.



Note

In Windows Server “Longhorn” Beta 2, you cannot install all four service roles at once. Because of internal dependencies, you must not install the MSCEP on the same machine as the CA until the CA is installed and running. To install the MSCEP on the same machine as the CA, you must install the CA first, and then add the MSCEP as a service role.

1. In this example (Figure 9), in the **Specify Setup Type** window, select Enterprise, and then click Next.



Figure : CA Setup Type Selection Dialog Box

1. To specify the CA Type (Figure 10), select Subordinate CA, and then click Next.



Figure 10: CA Type Selection Dialog Box

1. To set up the private key (Figure 11), select Create a new private key, and then click Next.



Figure : Private Key Selection Dialog Box

1. To configure the cryptography for the CA (Figure 12), select a CSP from the list. Selecting the CSP defines the cryptographic provider and also the public key algorithm that is used by the CA. At this point, you will implicitly decide if a classic provider or a CNG provider is used. Providers without a hash (#) in their name are classic Cryptographic application programming interface (CAPI) CSPs, and providers with a hash (#) in their name are CNG providers.

For greater flexibility, choose the RSA#Microsoft Software Key Storage Provider. This is a CNG provider and gives you greater flexibility regarding the hash algorithm that is used by the CA. For more information, see the "Configuring the Cryptographic Algorithms used by the CA" section.

In Windows Server “Longhorn” Beta 2, using an RSA or DSA provider on a subordinate CA erroneously results in a key size of 1024. The default key size for this provider will be 2048 in future preliminary Windows Server “Longhorn” releases.

Select the hash algorithm from the list, and then click **Next**.



Figure : Selection of the CSP or Key Provider

1. To configure the CA name (Figure 13), set the **Common name for this CA**, for example, CA11, and then click Next.



Figure : Setting the CA Name

1. Choose the way you want to submit the subordinate CA certificate request to the parent CA (Figure 14). Either send it to the parent CA across the network or save the request as a file to get the certificate back from the parent CA manually.



Figure : Submitting or Saving the CA Certificate Request

1. Optionally, specify the location of the Certificate Database, and then click Next (Figure 15).

**Note** The **Use existing certificate database from previous installation at this location** option is only available if you have chosen to use an existing key in the **Setup private key** dialog box.



Figure : Selecting the Certificate Database Path

1. Verify all settings that you have configured, and then click Install (Figure 16).



Figure : Confirming the Role Installation

1. To finish the installation, click Close.

#### Adding a Role Service

The following steps illustrate how to add a role service. In this example, Web enrollment is used as an additional role service to a computer where a CA is already installed.

1. Log on to the Windows Server “Longhorn” with appropriate permissions. To add a CA to an Active Directory environment, you must have Enterprise Administrator permissions. Otherwise, local administrator permissions are adequate.
2. On the Start menu, select Administrative Tools, and then select Server Manager.
3. On the **Server Manager** console, select the Manage Roles node in the left pane.
4. In the right pane, click Add role services in the Active Directory Certificate Server section.
5. Mark the service roles to be installed, in this example, choose **Certification Authority Web Enrollment**.



Note

In Windows Server “Longhorn” Beta 2, you may see various errors while installing MSCEP on the same machine as the CA if the CA is not properly running. For more information, see Troubleshooting.

1. To add the required Web Server role services, click Add Required Role Services, and then click Next.
2. In this example, the Web enrollment service and the CA are installed on the same computer. After reading the introduction to Web Server, click Next.

If the CA is located on a different computer, you have to specify the CA computer in the wizard. If necessary, the targeting CA for Web enrollment can be changed at a later stage through the certdat.inc file.

1. Walk through the Add Role Services wizard by clicking Next and finally Install.

#### Removing Active Directory Certificate Services as a Server Role

Active Directory Certificate Services can include up to four role services as described previously in this document.

**To remove all installed role services such as the Certificate Authority or the Online Certificate Status Protocol from a Windows Server “Longhorn” at the same time**

1. Log on to the Windows Server “Longhorn” with Enterprise Administrator permissions to remove an Enterprise CA. Log on to the Windows Server “Longhorn” as local Administrator to remove a Stand-alone CA.



Important

Technically, it is possible to remove an Enterprise CA while logged on as local Administrator. This is because a local Administrator always has full control on a computer.

However, when you remove an Enterprise CA, Active Directory is also affected as part of the removal procedure. If the account that is used to remove the CA does not have Enterprise Administrator permissions in Active Directory, PKI–related objects will remain in the configuration container. In case of auto enrollment, for example, clients will think that the uninstalled CA is still operational because it does exist in the Active Directory configuration.

1. On the Start menu, select Administrative Tools, and then select Server Manager.
2. On the **Server Manager** console, select the Manage Roles node in the left pane.
3. On the Action menu, select Remove Roles. The Remove Roles Wizard appears.
4. If the **Before you Begin** window appears, click Next.
5. In the list of roles, click to clear the Active Directory Certificate Server check box.
**Note** In Windows Server “Longhorn” Beta 2, the selection logic to remove a role is reversed. The final version of Windows Server “Longhorn” will require a check mark for those roles that have to be removed from the server.
6. To uninstall the Certificate Services role including all its role services, click Remove.
7. The server might have to be restarted to finalize the role removal procedure. To close the **Removal Results** screen, click Close.

#### Removing Role Services from Active Directory Certificate Services

Instead of removing the Active Directory Certificate Server role from a Windows Server Longhorn, you could also remove individual role services.

In Windows Server “Longhorn” Beta 2, a role cannot exist unless it contains at least one role service, therefore, only the second, third, and fourth Active Directory Certificate Server–related role service installed on a Windows Server “Longhorn” can be removed through this mechanism. To remove the last role service from a server, you must remove the role instead. In this case, it is not important which one the last role is. This may be changed in the next Windows Server “Longhorn” version or in the final release.

**To remove an Active Directory Certificate Server–related role service**

1. Log on to the Windows Server “Longhorn” with appropriate permissions.
2. On the Start menu, select Administrative Tools, and then select Server Manager.
3. On the **Server Manager** console, select the Manage Roles node in the left pane.
4. In the Active Directory Certificate Server section in the right pane, click Remove Role Services.
5. Click to clear the role services that should be removed from the server. At least one role service must remain to represent the Active Directory Certificate Server role.
**Note** In Windows Server “Longhorn” Beta 2, the selection logic to remove a role is reversed. The final release of Windows Server “Longhorn” will require a check mark for those roles that have to be removed from the server.
6. To uninstall the role services, click Remove.

**Note** If you have MSCEP or Web enrollment pointing to a local CA and you remove this CA, the remaining role services will be broken.

#### Role Service Default Settings

To install a role service, it is not required to walk through all dialog boxes of the Role Service Installation wizard. Almost all configuration settings have a default value so that you can immediately click the **Install** button once the role service is selected. Make sure that the default values meet your configuration requirements.

The following default settings apply for a server that is not joined to a domain.

|  |  |
| --- | --- |
| Configuration Option | Default Value |
| Role Services | Certificate Authority |
| Setup Type | Stand-alone |
| CA Type | Root CA |
| Set Up Private Key | Create a new private key |
| Configure Cryptography for CA | CSP: Microsoft Strong Cryptographic ProviderKey length: 2048Hash algorithm: SHA1 |
| CA Name | Common Name: [Hostname]-CADistinguished name suffix: <EMPTY> |
| Validity Period | 5 Years |
| Certificate Database | Certificate database location: %SYSTEMROOT%\system32\CertLogCertificate database log location: %SYSTEMROOT%\system32\CertLog |

The following default settings apply for a server that is joined to a domain.

|  |  |
| --- | --- |
| Configuration Option | Default Value |
| Role Services | Certificate Authority |
| Setup Type | Enterprise |
| CA Type | If a root CA is registered in the “Certification Authorities” container in the Active Directory configuration context, the default CA type is "Subordinate CA". If no root CA is available in the Active Directory configuration container, the default CA type is "root CA". |
| Set Up Private Key | Create a new private key |
| Configure Cryptography for CA | CSP: Microsoft Strong Cryptographic ProviderKey length: 1024Hash algorithm: SHA1 |
| CA Name | Common Name: [Domainname]-[Hostname]-CADistinguished name suffix: Active Directory Forest root namespace |
| Request Certificate from Parent CA | File name: %SYSTEMDRIVE%\[FQDN-Hostname]\_[DomainName]-[Hostname]-CA.req |
| Certificate Database | Certificate database location: %SYSTEMROOT%\system32\CertLogCertificate database log location: %SYSTEMROOT%\system32\CertLog |

#### Configuring Active Directory Certificate Services Using a CAPolicy.inf File

A number of specific configuration settings cannot be defined in the Role Service Configuration wizard. To set CA certificate extensions or define the renewal period of a CA certificate, for example, you must prepare a CAPolicy.inf file before the CA is set up or a CA certificate renewal is performed.

The CAPolicy.inf file applies only to the configuration of the CA; it is not used to configure MSCEP, OCSP, or the CAWE.

The CApolify.inf file must be available in the %SYSTEMROOT% directory before the CA role is installed on a Windows Server Longhorn. Make sure that you have local administrator permissions to create the file in the %SYSTEMROOT% directory.

The CAPolicy.inf file format for the Windows Server “Longhorn” CA is consistent with Windows Server 2003. For information about the Windows Server 2003 CAPolicy.inf file format, see
<http://technet2.microsoft.com/WindowsServer/en/Library/d6eab6a4-a680-40b0-9fde-4978be14ebf41033.mspx>

#### CDP and AIA Certificate Attributes

While it was necessary in previous Windows Server releases to create a CAPolicy.inf file to remove the CRL Distribution Point (CDP) and Authority Information Access (AIA) attributes from root certificates, the Windows Server “Longhorn” CA no longer includes those attributes for root certificates.

If you do not have requirements that would justify a CAPolicy.inf file, a root CA is set up properly without it.

#### Avoiding an Immediate Load of Default Certificate Templates During Setup

An Enterprise CA has 10 certificate templates assigned by default. Clients that are enabled for auto enrollment could start immediately to send certificate requests to the CA once it becomes available.

To avoid that immediate load on the CA, you have to set the following parameter in the certsrv\_server section.

LoadDefaultTemplates=0

In contrast to Windows Server 2003 SP1, the LoadDefaultTemplates parameter is not only interpreted by an enterprise root CA but since Windows Server “Longhorn” Release Candidate 1 (RC1), it also applies to enterprise subordinate CAs.

If the LoadDefaultTemplates parameter was set during installation, you have to assign certificate templates manually to the enterprise CA.

For example, to not load the default certificate templates during the setup of a CA, the CAPolicy.inf file would look like the following example.

[Version]

Signature="$Windows NT$"

[certsrv\_server]

LoadDefaultTemplates=0

#### Using Discrete Signatures for the CA Certificates or CA Certificate Requests

To support the PKCS#1 V2.1 signature format for CA certificate and CA certificate requests, a new parameter is available in the CAPolicy.inf file.

The parameter is required in two cases.

* To force a root CA to generate a self-signed root certificate that includes the PKCS#1 V2.1 signature format. In this case, the parameter has to be set in the capolicy.inf file at the root CA.
* To force a subordinate CA to generate a CA certificate request that includes the PKCS#1 V2.1 signature format. In this case, the parameter has to be set in the capolicy.inf file at the subordinate CA.

To apply the parameter at a CA, add the following line to the certsrv\_server section in the CAPolicy.inf file on Windows Server “Longhorn” Beta 2.

DiscreteSignatureAlgorithm=1

For example, to use the discrete signature on a Windows Server “Longhorn” post-Beta 2 installation during the setup of a CA, the CAPolicy.inf file would look like the following example.

[Version]

Signature="$Windows NT$"

[certsrv\_server]

DiscreteSignatureAlgorithm=1

#### Using Discrete Signatures for Issued Certificates

The previous section about the CAPolicy.inf file format showed how to enforce the use of the discrete signature during the certificate request generation for CA certificates.

This section describes how you can configure the CA to issue certificates that carry the PKCS#1 V2.1 signature format.

A special registry key can be set for a CA so that every certificate is issued with a discrete signature regardless of whether the certificate request was also signed with such a signature.

To set the Registry key, local administrator permission must be on the computer that has the CA installed. Carry out the following commands at a command-line prompt.

certutil -setreg ca\csp\DiscreteSignatureAlgorithm 1

net stop certsvc & net start certsvc

### Troubleshooting

This section provides troubleshooting information for Windows Server “Longhorn” Beta 2 issues.

#### Active Directory Certificate Services service terminated with service-specific error 2148081683 (0x80092013)

After installing and starting an enterprise CA, the Certificate Services service stops immediately and the following message is logged in the Global System event log: The Active Directory Certificate Services service terminated with service-specific error 2148081683 (0x80092013). At the same time, you receive an error in the Global Application Log: Active Directory Certificate Services did not start: Could not load or verify the current CA certificate. <CANAME> The revocation function was unable to check revocation because the revocation server was offline. 0x80092013 (-2146885613).

To work around the error, ensure that the CRL is accessible for the Local System account on the computer that runs the CA. In contrast to Windows 2000 and Windows Server 2003 where the CA used to run with full Local System privileges, a Windows Server “Longhorn” CA runs with stripped down privileges. To see the actual privileges of the CA, carry out the following command at a command-line prompt.

sc qpriv certsvc

To troubleshoot the issue, see "Enabling CAPI2 logging to troubleshoot chain validation errors".

You can generally translate error numbers with the certutil program, for example:

certutil -error 0x80092013

#### Web enrollment support cannot be installed on a different machine than the Certification Authority

If you are installing Web enrollment services on a dedicated computer, you may not see the target CA in the “Specify CA for Web Enrollment Services” dialog box. After selecting the CA Name option and clicking the Browse button, only the CAs that are actually registered appear in the Enrollment Services configuration container in Active Directory. If you have not installed the target CA with Enterprise permissions, the CA object might not appear in this container.

To fix the problem and register the CA properly in Active Directory, you must uninstall and reinstall the target CA.

## Upgrade

This section describes the supported upgrade paths from earlier Windows Certificate Services installations.

### Overview and Requirements

The following matrix for upgrade is supported with Windows Server “Longhorn” post-Beta 2.

|  |  |  |  |
| --- | --- | --- | --- |
| **Windows Version** | **SKU** | **Upgrade to Windows “Longhorn” SKU** | **Comments** |
| Standard Edition | Enterprise Edition | Data Center |
| NT4 | All SKUs | No | No | No | Not supported |
| Windows Server 2000 | SP4 | No | No | No |  |
| Advanced Server SP4  | No | No | No |  |
|  | Data Center SP4 | No | No | No |  |
| Windows Server 2003 | SP1, R2 | Yes | Yes | No | Windows Server 2003 RTM upgrade is not supported. |
| Enterprise Edition SP1, R2  | No | Yes | No | Windows Server 2003 RTM upgrade is not supported. |
| Data Center Edition | No | No | Yes |  |
| Itanium 64 | No | No | No | Active Directory Certificate Services is not supported on Windows Server “Longhorn” Itanium SKU. |

This table applies to both x86 and x64 stock keeping units (SKUs). Cross-architecture upgrades are not supported (that is, upgrades from x86 to x64).

### Scenario

Upgrade scenarios are not supported for Windows Server “Longhorn” Beta 2. Upgrading an existing CA to a Windows Server “Longhorn” computer will be supported in future releases of Windows Server Longhorn.

For information about migrating an existing CA to a Windows Server “Longhorn” computer, see the Microsoft Knowledge Base article at
http://support.microsoft.com/?kbid=298138

### Configuration

Upgrading an existing Windows server operating system is not yet supported for Windows Server Longhorn. Upgrades will be supported in future preliminary releases.

Detailed information about upgrading an existing Windows CA to Windows Server “Longhorn” will be provided in an updated version of this document after the release of Windows Server “Longhorn” Beta 2.

### Troubleshooting

Detailed upgrade troubleshooting steps will be provided in an updated version of this document after the release of Windows Server “Longhorn” Beta 2.

## Configuring the Cryptographic Algorithms used by the CA

As described in "Advanced Cryptography Support", the Windows Server “Longhorn” CA is able to also generate certificates that require alternate cryptography algorithms to RSA such as ECC.

Important Until you have a good understanding of how to enable the existing operating systems and applications in your environment with the new cryptography algorithms, you should use the default RSA asymmetric algorithm and SHA1 hash algorithm**.**

### Configuration

The Windows Server “Longhorn” CA supports changing the Cryptographic Provider and the asymmetric and the symmetric algorithm that is already installed and operational. In Windows versions earlier than Windows Server Longhorn, changing any of those parameters once the CA is installed is not supported. This functionality allows switching from classic cryptographic algorithms to CNG algorithms, for example.

The following table illustrates which registry key under the HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\{CAname}\CSP registry hive applies to which scenario. A check mark means that the value may be changed; a boxed check mark means that the value is required but must not be changed. The algorithm names that are supported are enclosed in parentheses.

|  |  |
| --- | --- |
| Registry Key | CA Certificate Hash and Issued Certificates |
|  | CAPI1 | CNG |
| Provider | 🗹 | 🗹 |
| ProviderType | 🗹 | 🗹 |
| HashAlgorithm | ✓ (SHA1, MD2, MD4, MD5) |  |
| CNGPublicKeyAlgorithm |  | 🗹 |
| CNGHashAlgorithm |  | ✓ (SHA1, MD2, MD4, MD5, SHA256, SHA384, SHA512) |

You cannot change the provider or provider type after the CA has been set up. The hash algorithms that can be used must be supported by the provider that is already configured in the registry.

For classic CAPI1 providers, no registry key for the public key algorithm exists. This is because for those providers, the public key algorithm is always implicit. Except for the Microsoft Base Digital Signature Standard (DSS) Cryptographic Provider where the default public key algorithm is DSA, all other classic CAPI1 providers use RSA as their default public key algorithm.

If you are changing the hash algorithm that is used to issue new certificates, you should understand where this change applies.

* In case of a root CA, the changed hash algorithm will be used to issue a new root CA certificate and also to sign certificates that are issued by this root CA. Note that you have to renew the root CA certificate and sign it with the new algorithm.
* In case of a subordinate CA, the change applies only for certificates that are issued by this CA. The change does not apply to the CA certificate because it is signed by the parent CA.

For example, if you have set up the CA with the Microsoft Strong Cryptographic Provider and an MD5 hash algorithm, the registry hive would look like the following configuration.

[HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\{CAname}\CSP]

"ProviderType"=dword:00000001

"Provider"="Microsoft Strong Cryptographic Provider"

"HashAlgorithm"=dword:00008003

If you have configured the Microsoft Software Key Storage Provider# ECDSA\_P521 CSP with a SHA512 hash algorithm, your registry configuration would look like the following example.

[HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\{CAname}\CSP]

"ProviderType"=dword:00000000

"Provider"="Microsoft Software Key Storage Provider"

"CNGPublicKeyAlgorithm"="ECDSA P521"

"CNGHashAlgorithm"="SHA512"

**To change the hash algorithm to a classic CAPI1 provider**

1. Log on to the Windows Server “Longhorn” CA with local administrator permissions.
2. Determine the CSP that is currently used by your CA by typing this command at a command-line prompt.

certutil -getreg ca\csp\Provider

1. Based on the resulting information from step 2, determine which hash algorithms are supported by the currently used CSP by typing this command at a command-line prompt.

certutil -v -csplist > csp.txt

1. Open the csp.txt file with Microsoft Notepad and search for the provider name that you have determined.
2. The information under the Provider name will provide you with the information to configure the hash algorithm. The section in the csp.txt file will look like the following text.

Provider Name: Microsoft Strong Cryptographic Provider

Provider Type: 1 - PROV\_RSA\_FULL

SHA-1 (Secure Hash Algorithm (SHA-1))

dwDefaultLen=160 dwMinLen=160 dwMaxLen=160

CALG\_SHA1

Algorithm Class: 0x8000(4) ALG\_CLASS\_HASH

Algorithm Type: 0x0(0) ALG\_TYPE\_ANY

Algorithm Sub-id: 0x4(4) ALG\_SID\_SHA1

The important information is found in the Algorithm Class, Algorithm Type and Algorithm Sub-id lines. The sum of all three values is the hash algorithm ID that you have to put in the registry at the CA. In this sample, the ID for the HashAlgorithm is 0x8004.

1. To finally change the hash algorithm, type the following command at the command-line prompt.

certutil -setreg ca\csp\HashAlgorithm 0x8004



Note

You can only change the HashAlgorithm in the CSP hive. You must not change the provider or provider type.

1. After the change, restart the CA. The new algorithm is used to sign issued certificates. Remember that a root CA issues the CA certificate to itself so that the change applies after the next renewal of the CA certificate. To verify the changed hash algorithm, issue a new certificate from the CA where you have applied the configuration change.

Instead, if you have decided to use a CNG provider as a hash algorithm, follow these steps.

1. Log on to the Windows Server “Longhorn” CA with local administrator permissions.
2. Determine the CSP that is currently used by your CA by typing this command at a command-line prompt.

certutil -getreg ca\csp\Provider

1. Based on the resulting information from step 2, determine which hash algorithms are supported by the currently used CSP by typing this command at a command-line prompt.

certutil -v -csplist > csp.txt

1. Open the file with Notepad and search for the provider name that you have determined in step 2.
2. The information under the Provider name will show you the hash algorithms that are supported by the current provider. The section in the csp.txt file will look like the following text.

Provider Name: Microsoft Software Key Storage Provider

 Hash Algorithms:

 MD2

 BCRYPT\_HASH\_INTERFACE -- 2

 NCRYPT\_HASH\_OPERATION -- 2

 MD4

 BCRYPT\_HASH\_INTERFACE -- 2

 NCRYPT\_HASH\_OPERATION -- 2

 MD5

 BCRYPT\_HASH\_INTERFACE -- 2

 NCRYPT\_HASH\_OPERATION -- 2

 SHA1

 BCRYPT\_HASH\_INTERFACE -- 2

 NCRYPT\_HASH\_OPERATION -- 2

 SHA256

 BCRYPT\_HASH\_INTERFACE -- 2

 NCRYPT\_HASH\_OPERATION -- 2

 SHA384

 BCRYPT\_HASH\_INTERFACE -- 2

 NCRYPT\_HASH\_OPERATION -- 2

 SHA512

 BCRYPT\_HASH\_INTERFACE -- 2

 NCRYPT\_HASH\_OPERATION -- 2

1. To finally change the hash algorithm, use the provider name from step 5 and type the following command, for example:

certutil -setreg ca\csp\CNGHashAlgorithm SHA512



Note

You can only change the CNGHashAlgorithm in the CSP hive. You must not change the provider, provider type, or CNGPublicKeyAlgorithm.

1. After the change, restart the CA. The new algorithm is used to sign issued certificates. Remember that a root CA issues the CA certificate to itself so that the change applies after the next renewal of the CA certificate. To verify the changed hash algorithm, issue a new certificate from the CA where you have applied the configuration change.

## Certificate Templates

This section describes the additional configuration settings that can be defined for certificate templates.

### Overview and Requirements

Certificate templates provide a practical way to implement certificate enrollment in a managed Active Directory environment with Enterprise CAs. The CA administrator can define the blueprint for certificates that are enrolled from Enterprise CAs.

Historically, static V1 certificate templates have been introduced with Windows 2000. With Windows Server 2003, customization was introduced with V2 certificate templates. With Windows Server Longhorn, more certificate templates and certificate template properties compared to the Windows Server 2003 templates became available. The new template types in Windows Server “Longhorn” are called V3 templates.

|  |  |  |
| --- | --- | --- |
|  | Windows version required to modify a template | Windows version of the CA where the template can be assigned |
| V1 template | n/a since V1 templates are static | Windows 2000 Enterprise EditionWindows Server 2003 Enterprise EditionWindows Server Longhorn |
| V2 template | Windows Server 2003Windows XPWindows Server Longhorn | Windows Server 2003 Enterprise EditionWindows Server “Longhorn” Enterprise Edition |
| V3 template | Windows Server Longhorn | Windows Server “Longhorn” Enterprise Edition |

Because of dependencies to the underlying operating system, Windows Server “Longhorn” templates can only be assigned to CAs that are running on a Windows Server Longhorn. Only Windows Vista client computers and Windows Server “Longhorn” computers can enroll for V3 certificate templates. V3 templates are not available in CAWE.

One important change in Windows Server “Longhorn” and Windows Vista is the support for the CNG (Suite-B). With Suite-B algorithms, it is possible to use alternate and customized cryptographic algorithms for encryption and signing certificates.

Compared to Windows Server 2003 templates, a V3 is enhanced in the following ways.

These properties are new in the Cryptography tab.

* Support for asymmetric algorithms implemented by a Key Service Provider (KSP). By default, Windows implements the following algorithms: DSA, ECDH\_P256, ECDH\_P384, ECDH\_P521, ECDSA\_P256, ECDSA\_P384, ECDSA\_P521, and RSA.
* Support for hash algorithms implemented by a KSP; by default, Windows implements the following algorithms: MD2, MD4, MD5, SHA1, SHA256, SHA384, and SHA512.
* A discrete signature (PKCS#1 V2.1) can be required for certificate requests. Activating this option will force a client that uses the certificate auto-enrollment functionality or enrolls a certificate through the Certificates MMC Snap-In to generate a certificate request that carries a discrete signature. Selecting this option does not mean that a certificate that is issued from this template also carries a discrete signature. The setting applies to the certificate request only. Also, the setting is not relevant for certificate requests that are created with the certreq.exe command-line tool.
* The list of providers is filtered based on the minimum key size that was chosen.

These properties are new in the Request Handling tab.

* The Advanced Encryption Standard (AES) algorithm can be specified to encrypt private keys while they are transferred to the CA.
* For machine templates, read permissions on the private key can be added to the Network Service so that services like IIS have permission to use certificates and keys that are available in the computer’s certificate store. In previous versions of Windows, it is required to adjust permissions manually on the computer’s certificate store.
* The list of asymmetric algorithms is filtered based on the template purpose in the Request Handling tab.

### Scenario

Contoso.com has an interest to migrate from the currently used cryptographic algorithms to CNG so that support for ECC becomes available on Windows Vista and Windows Server “Longhorn” computers. The PKI department is providing V3 templates to Windows Vista and Windows Server “Longhorn” computers so that certificate request processing will use ECC algorithms to create new key material.

With the use of discrete signatures during certificate request processing, Windows Vista and Windows Server “Longhorn” computers will specify the key generation algorithm as property in the certificate request.

Finally, to achieve the highest security level for key archival, Contoso.com has decided to use the AES encryption algorithm to encrypt any private key material when it is transferred from the client to the CA.

### Configuration

If you have installed V2 certificates in your Active Directory forest, you may have to upgrade the existing templates and add the new V3 certificate templates. If you do not have any certificate templates, all V1, V2, and V3 certificate templates are added to the configuration container of your Active Directory forest.

Once you are upgrading the Active Directory schema to the Windows Server Longhornversion, the ACL of domain controller certificate templates is extended with an Access Control Entry (ACE) for read-only domain controllers.

#### Upgrading the Default Templates

Windows Server “Longhorn” adds two new default certificate templates to a Windows Server 2003 or Windows Server “Longhorn” Active Directory. One certificate is used for OCSP Response Signing and the second one is for Kerberos Authentication. Both certificate templates are added to Active Directory when you open the Certificate Templates MMC Snap-In for the first time on a Windows Server “Longhorn” computer or when you first add a Windows Server “Longhorn” CA to Active Directory.

Windows Server “Longhorn” certificate templates are independent from the Active Directory domain functional or forest level. You can work with certificate templates using any domain functional level or forest level.

If you upgrade the Active Directory schema to the Windows Server “Longhorn” version (adprep /forestprep), a new built-in security group for read-only domain controllers will be added to the Kerberos Authentication, Domain Controller Authentication, Directory Email Replication, and Domain Controller certificate template.

In Windows Server 2003 Active Directory where certificate templates have been already registered, 31 default templates exist. To add the Windows Server “Longhorn” certificate templates to Active Directory before a Windows Server “Longhorn” Enterprise CA was installed, perform the following steps. You do not have to upgrade manually if you have already installed a Windows Server “Longhorn” CA. The certificate template upgrade is part of the CA installation.

1. Log on to a Windows Server “Longhorn” with Enterprise Administrator permissions. Only Enterprise Administrators have the right to add objects to the CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=… container.
2. At a command-line prompt, type the following command to open the Certificate Templates MMC Snap-In, and then press Enter.

certtmpl.msc

1. Before the Certificate Templates MMC Snap-In opens, the following message appears.



To add the default Windows Server “Longhorn” certificate template to Active Directory, click **Yes**.

1. Click **OK** to confirm the message Windows successfully installed the new certificate templates.
2. After the Certificate Templates MMC Snap-In has opened, verify that the OCSP Response Signing and the Kerberos Authentication certificate templates appear in the list.

#### Connecting the Certificate Templates MMC Snap-In to a Specific Domain Controller

The Certificate Templates MMC Snap-In in Windows Server “Longhorn” allows connecting to a specific domain controller instead of using a random domain controller. This change was introduced to avoid random selection of a domain controller for read and write operations.

#### Creating V3 Certificate Templates

Windows Server “Longhorn” certificate templates (V3) are created by duplicating an existing V1, V2, or V3 certificate template. Windows Server 2003 certificate templates (V2) can be created by duplicating Windows Server Longhorn, Windows Server 2003, or Windows 2000 certificate templates.

Before enrolling certificates that use the new encryption and hash algorithms, carefully consider your migration strategy to use CNG. For more information, see “Advanced Cryptography Support”.



Note

To enroll certificates using a key provider instead of a CSP, you must use a V3 certificate template. The certificate enrollment agent in Windows Vista and later versions of Windows will not offer any key providers if a V1 or V2 certificate template was selected.

**To create and configure a new Windows Server “Longhorn” certificate template**

1. Log on to a Windows Server “Longhorn” with Enterprise Administrator permissions. Only Enterprise Administrators have the right to modify certificate templates by default.
2. Open the Certificate Templates MMC Snap-In or, at a command-line prompt, type

certtmpl.msc

1. Select an existing certificate template. On the Action menu, select Duplicate Template. The Duplicate Template dialog box appears.
2. Select Windows Vista, and then click OK.

#### Customizing Windows Vista Certificate Templates

Customizing V3 certificate templates works the same as in Windows Server 2003. Figures 17 and 18 illustrate the new options in V3 templates as described previously.



Allow services that run as network service to access the computer certificate store.

The AES encryption algorithm is used to protect the private key during key exchange.

Figure : New Certificate Template Options in the Request Handling Tab



Allows discrete signatures for certificate request processing. See note below!

Provides a list of new CNG algorithms

Provides a list of new CNG algorithms

Figure : New Certificate Template Options in the Cryptography Tab

Certification service providers that are available on the system.

Note In Windows Server “Longhorn” Beta 2, the PKCS#1 V2.1 signature format option is only available if the algorithm name is RSA (Figure 18). This is incorrect. You should be able to modify the option for all algorithm names. This will be corrected in a future preliminary version of Windows Server Longhorn.

#### Default Certificate Templates in Windows Server 2003 and Windows Server “Longhorn”

When you install a new enterprise CA, default certificate templates are automatically assigned to the Certificate Service except if you have set the LoadDefaultTemplates=0 parameter in the CApolicy.inf file.

The default certificate templates in Windows Server “Longhorn” are different from those in Windows Server 2003. The following table shows the differences.

|  |  |  |
| --- | --- | --- |
| Template Name | Windows Server 2003 | **Windows** Server “Longhorn”  |
| Administrator | ✓ | ✓ |
| Basic EFS | ✓ | ✓ |
| Computer | ✓ | ✓ |
| Directory Email Replication |  | ✓ |
| Domain Controller | ✓ |  |
| Domain Controller Authentication | ✓ |  |
| EFS Recovery Agent | ✓ | ✓ |
| Kerberos Authentication |  | ✓ |
| Subordinate Certification Authority | ✓ | ✓ |
| User | ✓ | ✓ |
| Web Server | ✓ | ✓ |

### Troubleshooting

This section provides troubleshooting information for issues related to configuring certificate templates.

#### certutil -template output is incomplete

If you create a list of certificate templates at a command-line prompt using certutil -template, you will recognize that Windows Vista certificate templates V3 are missing.

This behavior will occur if you are running an earlier version of the certutil program than the one provided with Windows Vista or Windows Server Longhorn. Only the Windows Vista or Windows Server “Longhorn” version of the certutil program also lists Windows Vista certificate templates.

#### certificate templates are not available

If you experience problems with the registration of certificate templates or if you have accidentally deleted some or all of the default templates, you can recreate the default templates with the following command.

regsvr32 /i:i /n %windir%\System32\certcli.dll

This command works in both Windows Server 2003 and Windows Server Longhorn. If you carry out the command in Windows Server 2003, default certificate templates for Windows 2000 and Windows Server 2003 are restored. If you carry out the command in Windows Server Longhorn, the Windows Server “Longhorn” certificates are also restored.

## Restricted Enrollment Agent

This section describes the way that an enrollment agent can enroll certificates.

### Overview and Requirements

Enrollment agents are one or more authorized individuals within an organization. The enrollment agent needs to be issued an Enrollment Agent certificate, which enables the agent to enroll for certificates on behalf of users. Enrollment agents are typically members of the corporate security, IT security, or help desk teams because these individuals have already been trusted with safeguarding valuable resources. In some organizations, such as banks that have many branches, help desk and security workers might not be conveniently located to perform this task. In this case, designating a branch manager or other trusted employee to act as an enrollment agent is required.

The Windows Server 2003 Enterprise CA does not provide any configurable means to control enrollment agents except from enrollment agents’ certificates enforcement. The enrollment agent certificate is a certificate containing the "Certificate Request Agent" application policy extension (OID=1.3.6.1.4.1.311.20.2.1).

The restricted enrollment agent is a new functionality that allows limiting the permissions enrollment agents have for enrolling on behalf of other users. On a Windows Server “Longhorn” Enterprise CA, an enrollment agent can be permitted for one or many certificate templates. For each certificate template, it is configurable for which users or security groups the enrollment agent can enroll on behalf of. You cannot constrain an enrollment agent based on a certain Active Directory organizational unit (OU) or container. As mentioned previously, you must use security groups. Note that the restricted Enterprise enrollment agent is not available on a Standard CA.

Figure 19 illustrates the combinations that are possible for the restricted enrollment agent. A single or multiple certificate templates can be assigned to an enrollment agent (or a group). Multiple restricted enrollment agents can share different certificates or use the same certificate template. The agent can be explicitly permitted or denied for single or multiple users or groups (Figure 19).



Figure : Combination of Agents, Templates, and Credentials

The restricted enrollment agent functionality is available through the Certificate Services user interface on an enterprise CA. At this stage, there is no support to configure the restricted enrollment agent from a script or through an API.

### Scenario

Contoso.com has many small offices around the globe. Registration authorities for smart cards are usually located in those offices to make smart cards instantly available to end users. In Windows Server Longhorn, the PKI architects of Contoso.com will be able to restrict enrollment agents so that enrollment is only possible for a certain certificate template. In Windows Server 2003, there was no way to permit an enrollment agent to enroll a certain group of smart card holders only.

Contoso.com has decided to create a security group for each registration authority and permit the enrollment agents of those registration authorities individually on the smart card logon certificate template.

By default, an enrollment agent is not restricted and is able to enroll for all users all kinds of certificate templates.

### Configuration

Before configuring restricted enrollment agents, you should create security groups in Active Directory. Depending on your restriction policy, you may have a security group for all enrollment agents in a registration authority and also a different security group for the users that are assigned to a registration authority. With those two security groups per registration authority, you are able to limit capabilities of the enrollment agents granularly.

With the restricted enrollment agent, you are restricting the templates and the users that an enrollment agent can enroll for.

If you have two registration authorities, for example, follow these steps to configure the security groups and the enrollment agent restrictions.

1. Log on with permissions to create security groups.
2. For the registration authority enrollment agents in registration authority 1, create one security group called RA1EnrollAgents and another security group called RA2EnrollAgents. Add the users that will act as enrollment agents. Choose the group type depending on your infrastructure. If all enrollment agents are members of the same domain, use global groups.
3. For users that belong to the registration authority 1, create a security group called RA1users, and for users in RA2, use RA2users. Add the users accordingly. Also, choose the group type depending on your infrastructure.
4. Log off and log on with CA Administrator permissions.
5. On the Start menu, select Administrative Tools, and then click Certification Authority. The Certification Authority MMC Snap-In opens.
6. Click the **Certification Authority** container in the left pane. On the **Action** menu, select Properties.
7. Click the Enrollment Agents tab.
8. Select the Restrict enrollment agents option.



Important

After starting the configuration of restricted enrollment agents, it is recommended that you save the restriction configuration by clicking the **Apply** button regularly. If you have not applied your restriction configuration and you click the "Do not restrict enrollment agents" option, your entire configuration in this tab will be lost.

1. In the **Enrollment agents** list box, select Everyone, and then click Remove.
2. In the Enrollment agents section, click Add.
3. In the Select User, Computer, or Group dialog box, type **RA1EnrollAgents**, and then click OK.



Note

It is intended behavior that multiple user, computer, or group selections are not possible in the advanced search dialog box. Since restricted enrollment agents will have a performance impact on the CA, you should add as few Active Directory accounts to the list of Enrollment agents as possible. You should also keep the list of accounts in the permissions list small. Instead of using user accounts, use group accounts in both lists.

1. In the Certificate Templates list box, select **<All>**, and then click the associated Remove button.
2. Click the Add button that is close to the Certificate Templates list box.
3. Select the certificate template(s) that you intend to make available to your enrollment agent, and then click OK.
4. In the Permissions section, select **Everyone**, and then click Remove.
5. In the Select User, Computer, or Group dialog box, type **RA1users**, and then click OK.
6. Repeat steps 10 and 11 to add the **RA2EnrollAgents**, add the same or a new template as described in steps 12 to 14, and repeat steps 15 and 16 to add the **RA2users**.
7. To finish your configuration, click OK.
8. Make sure that your Enrollment Agents hold valid enrollment agent certificates.

After performing these configuration steps, members of the RA1EnrollAgents security group can request certificates on behalf from the Contoso Smartcard Logon certificate template for the RA1users only. RA2EnrollmentAgents have only permissions to enroll on behalf of RA2users from the Contoso Smartcard Logon certificate template. Figure 20 illustrates the Enrollment Agents tab for the configuration described previously.



Figure : Enrollment Agents Configuration

To change the certificate template(s) for an enrollment agents group, select the appropriate entry in the Enrollment Agents list box, and then change the Certificate Template settings.

If you have nested groups, you can also explicitly deny permissions to not allow a certain group member in the main group. Also, you can deny individual members that are members in a security group. Similar to the normal behavior for ACLs, deny permissions supersede allow permissions. That means if a user has allow-permissions as a group member but has deny-permissions as a user, the user will have deny-permissions.

### Troubleshooting

This section provides troubleshooting information for issues related to configuring restricted enrollment agents.

#### Certificate templates do not appear in the Add certificate template dialog

If the CA properties dialog box is open and you are creating a new certificate template with the Certificate Templates MMC Snap-In during that time, the new certificate template does not appear in the list of certificates.

To fix this problem, close the Certification Authorities Properties dialog box and re-open it.

#### “No properties are available on this object.” when opening a V3 certificate template

When you attempt to open a V3 certificate template on a Windows Server 2003, Windows XP, or Windows 2000 computer, the General tab of the template properties will display the message “No properties are available on this object.”

You cannot open or modify V3 templates on computers that run an earlier Windows version than Windows Vista or Windows Server Longhorn.

## Restricted Certificate Managers

This section describes the way to define the entities that a certificate manager can enroll or revoke certificates for.

### Overview and Requirements

In Windows Server 2003, it is not possible to control certificate management granularly. A user that has certificate manager permissions on a Windows Server 2003 CA is able to approve and revoke certificates for all certificate types. This might be a problem for environments where role separation between certificate managers is required.

The restricted certificate manager functionality is available on a stand-alone or enterprise CA.

### Scenario

Contoso.com is using certificates for various purposes from their PKI. With Windows Server 2003, it was difficult for them to implement a good certificate management process for Secure Socket Layer (SSL) and code-signing certificates. Contoso.com runs many SSL servers where it is quite difficult for the certificate manager to decide on the issuance of pending requests. The certificate manager is removed from the distributed teams that run SSL servers. The same issue is true for certificate-signing certificates. It was time-consuming to check with the person who submitted a code-signing certificate request to verify whether the certificate request was correct.

With Windows Server Longhorn, Contoso is implementing restricted certificate managers so that selected people have the ability to issue and revoke certificates that are issued based on a certain certificate template. Contoso.com is implementing several security groups as Certificate Managers and several security groups for which the certificate managers have certificate management permissions. The logic is the same as for the restricted enrollment agent. See Figure 19 for the relationship between restricted certificate managers, templates, and users or groups.

At this stage, there is no support to configure the restricted certificate managers from a script or through an API.

### Configuration

Before configuring restricted certificate managers, you should create security groups in Active Directory. Depending on your restriction policy, you may have several security groups that are permitted on the same or different certificate templates. For each certificate template, different user accounts or security groups can be explicitly permitted or denied.

With the restricted certificate manager, you are restricting the templates and the users that a certificate manager can manage certificates for.

If you have three groups of certificate managers that issue certificates for two templates, for example, follow these steps to configure the security groups and certificate manager restrictions.

1. Log on with permissions to create security groups.
2. For code signing, create a security group called CertManCodeSign. Add the users that will act as certificate managers for code-signing certificates. Create a security group CertHoldersCodeSign and add the users that will submit certificate requests for code-signing certificates.
3. Create a security group called CertManSSL. Add the users that will act as certificate managers for SSL certificates. Create a security group CertHoldersSSL and add the users or computers that will submit SSL certificate requests.
4. Log off and log on with Enterprise Administrator permissions to prepare the certificate templates.
5. On the Start menu, select Administrative Tools, and then click Certification Authority. The Certification Authority MMC Snap-In opens.
6. Expand the **Certification Authority** node in the left pane, and then select the Certificate Templates container. On the Action menu, click Manage. The list of certificate templates in your Active Directory appears.
7. In the right pane of the **Certificate Templates** MMC Snap-In, select the Code Signing certificate template. On the **Action** menu, click Properties.
8. Click the Security tab.
9. To permit the **CertHoldersCodeSign** security group for enrollment on this certificate template, click Add.
10. In the Select Users, Computers, or Groups dialog box, type the name of the security group, in this sample, **CertHoldersCodeSign**, and then click OK.



Note

It is intended behavior that multiple user, computer, or group selections are not possible in the advanced search dialog box. Since restricted Certificate Managers will have a performance impact on the CA, you should add as few Active Directory accounts as possible to the list of Enrollment agents. You should also keep the list of accounts in the permissions list small. Instead of using user accounts, use group accounts in both lists.

1. While the **CertHoldersCodeSign** entry is elected in the Group or user names listbox, allow Enroll in the lower list box.
2. Repeat steps 9–11 for the **CertHoldersSSL** security group, and then click OK.
3. Make sure that you leave the Authenticated Users with Read permissions in the upper list box; otherwise, the CA is no longer able to read the certificate template.
4. Close the **Certificate Templates** MMC Snap-In and return to the **Certification Authority** MMC Snap-In.
5. While the Certificate Templates container is selected, click Action, click New, and then click Certificate Template to Issue.
6. Select the Code Signing certificate, and then click OK. The Web Server certificate template should be part of the certificate templates that are assigned to a CA by default.
7. Log off and log on with CA manager permissions.
8. On the Start menu, select Administrative Tools, and then click Certification Authority. The Certification Authority MMC Snap-In opens.
9. Click the **Certification Authority** container in the left pane. On the **Action** menu, select Properties.
10. Click the Security tab.
11. Click the Add button and type the name of your newly created restricted certificate manager security groups, such as CertManCodeSign and CertManSSL, and then click OK.
12. In the Group or user names list box, select **CertManCodeSign**. Select Allow permissions to Issue and Manage Certificates, and then remove the permission to Request Certificates. Repeat this step for the security group **CertManSSL**, and then click Apply.
13. Click the Certificate Managers tab.
14. Select Restrict certificate managers, and then verify that the newly permitted certificate managers appear in the list.



Important

After starting the configuration of restricted certificate managers, it is recommended that you save the restriction configuration by clicking the **Apply** button regularly. If you have not applied your restriction configuration and you click the "Do not restrict certificate managers" option, your entire configuration in this tab will be lost.

1. In the **Certificate Managers** list, select the **CertManCodeSign** entry.
2. In the Certificate Templates list box, select **<All>**, and then click the associated Remove button.
3. Click Add, and then select the certificate template(s) that you intend to make available to users. In this case, click the Code Signing certificate template, and then click OK.
4. In the Permissions section, select **Everyone**, and then click Remove.
5. Click the Add button associated with the **Permissions** list box. In the Select User, Computer, or Group dialog box, type **CertHoldersCodeSign** in this example, and then click OK.



Note

It is intended behavior that multiple user, computer, or group selections are not possible in the advanced search dialog box. Since restricted Certificate Managers will have a performance impact on the CA, you should keep the list of accounts in the permissions list small. Instead of using user accounts, use group accounts in both lists.

1. In the Certificate Managers list box, select the **CertManSSL** entry.
2. In the Certificate Templates list box, select **<All>**, and then click the associated Remove button.
3. Click Add, and then select the certificate template(s) that you intend to make available to users. In this case, click the Web Server certificate template, and then click OK.
4. In the Permissions section, select **Everyone**, and then click Remove.
5. Click the Add button associated with the permissions list box. In the Select User, Computer, or Group dialog box, type **CertHoldersSSL**, in this example, and then click OK.
6. To finish your configuration, click OK.

After performing these configuration steps, members of the CertManCodeSign security group can only approve and revoke certificates that are issued with the Web Server certificate template. The only user group that can enroll from the Web Server certificate template is the CodeSignCertHolder.

Figure 21 illustrates how the restricted Certificate Managers tab looks after you have completed the previous configuration steps.

 

Figure : Restricted Certificate Managers Tab after Configuration

### Troubleshooting

This section provides troubleshooting information for issues related to configuring restricted certificate managers.

#### The Certification Authorities properties dialog does not match the screenshots from above

If you look at the Certification Authority properties dialog box in Windows Server 2003, you will see the same dialog box that was available in Windows Server 2003. You have to be logged on to a Windows Server “Longhorn” computer to maintain restricted Certificate Managers.

#### You cannot add or remove certificate managers from the “Certificate Managers” dialog

To change the list of certificate managers that appear in the Certificate Managers tab, use the Security tab.

#### A SID appears in the Certificate Managers or Permissions list box instead of the user or group name

If a security identifier (SID) appears as user account or group, the system cannot resolve the account that corresponds to the SID that is maintained in the ACL. There are various reasons for this behavior.

One reason is that the user or group was deleted from Active Directory while the SID is still in the restricted certificate managers ACL. In this case, you can safely remove the SID from the list of Certificate Managers or Permissions. You may also consider revoking certificates that have been enrolled to this user.

Another reason is that the CA is not able to contact a domain controller from the domain that is hosting the user or group account. If it is a trusted domain, you can check the trust relationship between the domain where the CA is a member and the trusted domain.

## Key Archival and Recovery

This section describes how to recover private keys in Windows Server “Longhorn” and how to use stronger encryption algorithms for private key protection.

### Overview and Requirements

The key recovery functionality was introduced in the Windows Server 2003 Enterprise CA. Key archival is only available on Enterprise CAs.

Windows Server “Longhorn” slightly changes how archived keys are archived and recovered. With Windows Server 2003, a dialog box–based key recovery tool is available with the Resource Kit. Windows Server “Longhorn” does not provide a Resource Kit, so the only way to recover keys is with the certutil program.

A second change is that Suite-B algorithms are supported to encrypt the private keys in the CA database.

### Scenario

Contoso.com has always been interested in keeping its PKI as secure as possible. Because stronger encryption algorithms are available in Windows Server Longhorn, Contoso.com has decided to change the encryption algorithm that is used by default to protect private keys that are stored in the database of the CA.

### Configuration

The following sections describe how to recover private keys from the command line and how to change the algorithm that is used to encrypt private keys in the CA database.

#### Performing Key Recovery at the Command Line

Key recovery retrieves the private key binary large object (BLOB) from the CA database and recovers it into a protected .pfx file. The .pfx file can be imported by a user who has previously lost the private key.

For more information about retrieving and recovering private keys with the certutil program, see the Microsoft TechNet Web site at
<http://technet2.microsoft.com/WindowsServer/en/Library/b6d777d3-1f94-435e-a8a0-75f8ef198c701033.mspx>

For an example implementation of key archival and recovery, see the Microsoft TechNet Web site at
<http://technet2.microsoft.com/WindowsServer/en/Library/9216103d-91c6-40da-a370-f95ccf4beaca1033.mspx>



Note

The krt.exe command-line tool available in the Windows Server 2003 Resource Kit was not tested with the Windows Server “Longhorn” Beta 2 release. Therefore, you should not use this tool to perform key recovery with “Longhorn” Server Beta 2.

#### Changing Cryptographic Algorithms for Key Exchange and Key Archival

Windows versions prior to Windows Server “Longhorn” did not have the capability to change the algorithm that is used to create the key exchange certificate or to create the symmetric key that is used for key archival. With Windows Server Longhorn, you can change the algorithm and key size in certain scenarios. The following table illustrates which registry keys in the HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\{CAname} are required to build the key exchange certificate or the symmetric key algorithm. A check mark means that the value may be changed; a boxed check mark means that the value is required but cannot be changed. The algorithm names that are supported are enclosed in parentheses.

Note that the provider and the provider type apply for both purposes. That means you must choose the key archival provider depending on your choice for the key exchange provider.

|  |  |  |
| --- | --- | --- |
|  | Key Exchange | Key Archival |
|  | CAPI1 | CNG | CAPI1 | CNG |
| EncryptionCSP\Provider | ✓ | ✓ | ✓ | ✓ |
| EncryptionCSP\ProviderType | ✓ | ✓ | ✓ | ✓ |
| EncryptionCSP\EncryptionAlgorithm |  |  | 🗹 (3DES) |  |
| EncryptionCSP\KeySize | ✓ | ✓ |  |  |
| EncryptionCSP\SymmetricKeySize |  |  | 🗹(168) | ✓ |
| EncryptionCSP\CNGPublicKeyAlgorithm |  | ✓(RSA, ECDH) |  |  |
| EncryptionCSP\CNGEncryptionAlgorithm |  |  |  | ✓(3DES, AES) |

##### Changing the CA Key Exchange Algorithm or its Key Size

The CA maintains an encryption key that is used when a private key needs to be transferred securely from a client computer to the CA for key archival. The key material for key exchange is created on demand when a client requests the public key from the CA.

Key exchange is part of the key archival process. For more information, see the section "Understanding Automatic Key Archival" in the document "Key Archival and Management in Windows Server 2003" at
<http://technet2.microsoft.com/WindowsServer/en/Library/6f5bb2ac-877e-47c3-8faa-f7dc1b15b11b1033.mspx>

The following steps are performed to transfer a private key securely from a client computer to the CA.

* Based on the key archival flag on the certificate template that is used for certificate enrollment, the client requests the CA’s encryption certificate from the CA.
* Based on the client’s request, the CA verifies whether it has a valid encryption key. If this is the first client or the encryption certificate has expired, the CA generates a new encryption certificate. It uses the algorithm from the Certificate Service configuration in the registry (CA\EncryptionCSP) and the CA Exchange certificate template to build the certificate request.
* Once the CA has enrolled for the key exchange certificate, it uses this certificate for all key exchange operations for at most seven days. This is the default validity time as configured in the CA Exchange template.
* The CA key exchange certificate is sent to the client.
* The client generates a symmetric key. If a Windows Vista certificate template is used, the client will check for the algorithm that should be used. If the "Use AES for key archival" option is selected in the request handling tab, it uses the AES algorithm with a key length of 256; otherwise, the 3DES algorithm is used.
* The client encrypts its private key with the symmetric key as generated in the previous step. The symmetric key is protected with the public key from the CA Exchange certificate.
* The CA uses its private key to decrypt the symmetric key that was generated by the client. It then decrypts the client’s private key with the symmetric key.
* It then re-encrypts it with the symmetric algorithm set in the registry and encrypts this key to the key recovery agent (KRA).

**To use the default public key algorithm and configure the key size for the exchange key for a classic CAPI1 provider**

1. Log on to the Windows Server “Longhorn” CA with local administrator permissions.
2. Create a file of the certificate service providers that are available on your computer by using the following command.

certutil -v -csplist > csp.txt

1. Use Notepad to open the csp.txt file. Search for RSA\_KEYX to find a provider that supports the default key exchange algorithm.
2. After you have found the correct RSA\_KEYX algorithm, verify whether the algorithm supports the key size that you intend to use. Note that different providers support different key sizes for the RSA\_KEYX algorithm.
3. Scroll to find the provider name and type that supports the algorithm that you have found.

The following list shows the common providers and types that can be used with the RSA\_KEYX algorithm.

|  |  |  |
| --- | --- | --- |
| Provider | Type | Min-Max Key len |
| Microsoft Base Cryptographic Provider v1.0 | 1 | 512 - 1024 |
| Microsoft Enhanced Cryptographic Provider v1.0 | 1 | 384 - 16384 |
| Microsoft Enhanced RSA and AES Cryptographic Provider | 24 | 384 - 16384 |
| Microsoft RSA SChannel Cryptographic Provider | 12 | 384 - 16384 |



Note

The same provider is used to generate keys for key exchange and key archival. Depending on your requirements for the key archival algorithm, you have to change the appropriate algorithm at this stage.

1. To configure the provider and set the key size, use the provider and provider type that you have determined and set the key size with the following command. For example, carry out these commands.

certutil -setreg ca\EncrpytionCSP\Provider "Microsoft Enhanced RSA and AES Cryptographic Provider"

certutil -setreg ca\EncrpytionCSP\ProviderType 24

certutil -setreg ca\EncrpytionCSP\Keysize 4096

You have now configured the CA to use a classic CAPI1 provider to generate the key exchange certificate with the default RSA algorithm where a key size of 4096 bytes is used.

1. To verify your change, type the following command at a command-line prompt.

certutil -cainfo xchg

The command will show you the current key exchange certificate or will generate a new one if none is available.

If you notice that the key exchange certificate does not mirror the new configuration settings, an old key exchange certificate existed. This might be because the CA issues key exchange certificates on demand and keeps them for seven days. To enable the new configuration, you must revoke any existing key exchange certificate. When a key exchange certificate is needed the next time, the CA will apply the new configuration settings with this certificate.

**To configure the algorithm and the key size for the exchange key for a CNG provider**

Note Changing the CNG algorithm for encryption keys is not yet supported in Windows Server “Longhorn” Beta 2.

1. Log on to the Windows Server “Longhorn” CA with local administrator permissions.
2. List the certificate service providers that are available on your computer by using the following command.

certutil -v -csplist > csp.txt

The version of the certutil program that is available in Windows Server “Longhorn” Beta 2 does not show the supported key sizes for key storage providers. Later versions show the supported key sizes.

1. Use Notepad to open the csp.txt file. Search for **Microsoft Software Key Storage Provider**, which is the default Microsoft CNG provider.
2. Under **Provider**, search for **Asymmetric Encryption Algorithms** or **Secret Agreement Algorithms**. The section looks like the following text.

Asymmetric Encryption Algorithms:

 RSA

 BCRYPT\_ASYMMETRIC\_ENCRYPTION\_INTERFACE -- 3

 NCRYPT\_ASYMMETRIC\_ENCRYPTION\_OPERATION -- 4

 NCRYPT\_SIGNATURE\_OPERATION -- 10 (16)

 Secret Agreement Algorithms:

 DH

 BCRYPT\_SECRET\_AGREEMENT\_INTERFACE -- 4

 NCRYPT\_SECRET\_AGREEMENT\_OPERATION -- 8

 ECDH P256

 BCRYPT\_SECRET\_AGREEMENT\_INTERFACE -- 4

 NCRYPT\_SECRET\_AGREEMENT\_OPERATION -- 8

 NCRYPT\_SIGNATURE\_OPERATION -- 10 (16)

 ECDH P384

 BCRYPT\_SECRET\_AGREEMENT\_INTERFACE -- 4

 NCRYPT\_SECRET\_AGREEMENT\_OPERATION -- 8

 NCRYPT\_SIGNATURE\_OPERATION -- 10 (16)

 ECDH P521

 BCRYPT\_SECRET\_AGREEMENT\_INTERFACE -- 4

 NCRYPT\_SECRET\_AGREEMENT\_OPERATION -- 8

 NCRYPT\_SIGNATURE\_OPERATION -- 10 (16)

1. To actually configure the CNG key provider, carry out the following commands, for example:

certutil -setreg ca\EncrpytionCSP\Provider "Microsoft Software Key Storage Provider"

certutil -setreg ca\EncrpytionCSP\ProviderType 0x0

certutil -setreg ca\EncrpytionCSP\KeySize 256

certutil -setreg ca\EncrpytionCSP\CNGPublicKeyAlgorithm "ECDH P256"

The ProviderType equals NULL indicates that a CNG algorithm is used instead of a classic algorithm.

1. To verify your change, type the following command at a command-line prompt.

certutil -cainfo xchg

The command will show you the current key exchange certificate or will generate a new one if none is available.

##### Changing the Key Archival Algorithm for the CA

In Windows Server Longhorn, you can also change the algorithm that is used to protect archived keys. As documented in the "Key Archival and Management in Windows Server 2003" document, the CA generates an individual symmetric key for every archived key. This key is encrypted with one or many KRA public keys.

Generally, you can change the algorithm that is used for key archival to a classic or to a Suite-B algorithm. Depending on the provider, different registry values in the HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\{CAname}\EncryptionsCSP registry key are relevant.

|  |  |  |
| --- | --- | --- |
|  | Classic CAPI1 Provider | CNG Provider |
| Provider | Name of the provider | Name of the provider |
| ProviderType | Provider ID | 0x0 |
| KeySize | Hash algorithm ID | unused |
| CNGEncryptionAlgorithm | Unused | Algorithm name |
| SymmetricKeySize | Unused | KeySize |

**To create the symmetric key algorithm with a classic CAPI1 provider**

1. Log on to the Windows Server “Longhorn” CA with local administrator permissions.
2. Determine the information about the provider that is currently in use by using the following command.

certutil -v -getreg ca\EncryptionCPS\Provider

1. List the certificate service providers that are available on your computer by using the following command.

certutil -v -csplist > csp.txt

1. Use Notepad to open the csp.txt file. Search for the provider name that you have determined in step 2.
2. Under **Provider**, select an algorithm that has **ALG\_CLASS\_DATA\_ENCRYPT** as **Algorithm Class**. If your currently configured provider is the **Microsoft Enhanced RSA and AES Cryptographic Provider**, for example, you would have a choice between the following algorithms.

Provider Name: Microsoft Enhanced RSA and AES Cryptographic Provider

Provider Type: 24 - PROV\_RSA\_AES

 RC2 (RSA Data Security's RC2)

 dwDefaultLen=128 dwMinLen=40 dwMaxLen=128

 CALG\_RC2

 Algorithm Class: 0x6000(3) ALG\_CLASS\_DATA\_ENCRYPT

 Algorithm Type: 0x600(3) ALG\_TYPE\_BLOCK

 Algorithm Sub-id: 0x2(2) ALG\_SID\_RC2

 RC4 (RSA Data Security's RC4)

 dwDefaultLen=128 dwMinLen=40 dwMaxLen=128

 CALG\_RC4

 Algorithm Class: 0x6000(3) ALG\_CLASS\_DATA\_ENCRYPT

 Algorithm Type: 0x800(4) ALG\_TYPE\_STREAM

 Algorithm Sub-id: 0x1(1) ALG\_SID\_RC4

 DES (Data Encryption Standard (DES))

 dwDefaultLen=56 dwMinLen=56 dwMaxLen=56

 CALG\_DES

 Algorithm Class: 0x6000(3) ALG\_CLASS\_DATA\_ENCRYPT

 Algorithm Type: 0x600(3) ALG\_TYPE\_BLOCK

 Algorithm Sub-id: 0x1(1) ALG\_SID\_DES

 3DES TWO KEY (Two Key Triple DES)

 dwDefaultLen=112 dwMinLen=112 dwMaxLen=112

 CALG\_3DES\_112

 Algorithm Class: 0x6000(3) ALG\_CLASS\_DATA\_ENCRYPT

 Algorithm Type: 0x600(3) ALG\_TYPE\_BLOCK

 Algorithm Sub-id: 0x9(9) ALG\_SID\_3DES\_112

 3DES (Three Key Triple DES)

 dwDefaultLen=168 dwMinLen=168 dwMaxLen=168

 CALG\_3DES

 Algorithm Class: 0x6000(3) ALG\_CLASS\_DATA\_ENCRYPT

 Algorithm Type: 0x600(3) ALG\_TYPE\_BLOCK

 Algorithm Sub-id: 0x3(3) ALG\_SID\_3DES

 AES 128 (Advanced Encryption Standard 128-bit)

 dwDefaultLen=128 dwMinLen=128 dwMaxLen=128

 CALG\_AES\_128

 Algorithm Class: 0x6000(3) ALG\_CLASS\_DATA\_ENCRYPT

 Algorithm Type: 0x600(3) ALG\_TYPE\_BLOCK

 Algorithm Sub-id: 0xe(14) ALG\_SID\_AES\_128

 AES 192 (Advanced Encryption Standard 192-bit)

 dwDefaultLen=192 dwMinLen=192 dwMaxLen=192

 CALG\_AES\_192

 Algorithm Class: 0x6000(3) ALG\_CLASS\_DATA\_ENCRYPT

 Algorithm Type: 0x600(3) ALG\_TYPE\_BLOCK

 Algorithm Sub-id: 0xf(15) ALG\_SID\_AES\_192

 AES 256 (Advanced Encryption Standard 256-bit)

 dwDefaultLen=256 dwMinLen=256 dwMaxLen=256

 CALG\_AES\_256

 Algorithm Class: 0x6000(3) ALG\_CLASS\_DATA\_ENCRYPT

 Algorithm Type: 0x600(3) ALG\_TYPE\_BLOCK

 Algorithm Sub-id: 0x10(16) ALG\_SID\_AES\_256

1. Sum the values for **Algorithm Class**, **Algorithm Type**, and **Algorithm Sub-id** for the provider of your choice.
2. To use the AES 256 provider, for example, carry out the following commands.

certutil -setreg ca\EncrpytionCSP\EncyptionAlgorithm 0x6610

certutil -setreg ca\EncrpytionCSP\SymmetricKeySize 256

**Or, to create the symmetric key algorithm with a CNG provider**

1. Log on to the Windows Server “Longhorn” CA with local administrator permissions.
2. Determine the information about the provider that is currently in use by using the following command.

certutil -v -getreg ca\EncryptionCPS

1. Make sure that the provider type is set to 0x0 and make a note of the provider name. If the provider type is not zero, your current provider is not a CNG provider. Perform the steps to change the key exchange algorithm and its key size as documented in "Changing the CA Key Exchange Algorithm or its Key Size".
2. List the certificate service providers that are available on your computer by using the following command.

certutil -v -csplist > csp.txt

1. Use Notepad to open the csp.txt file. Search for the provider name that you have determined in step 3.
2. The output of the previous command will tell you the configuration details about algorithm of your interest. Look at the **Cipher Algorithms** in the **CryptEnumAlgorithms** section to find an appropriate algorithm. The provider names represent the values for the CNGEncryptionAlgorithm registry key. For example, if you want to change the algorithm that is used to generate the symmetric key from the default value 3DES to AES 192, carry out the following commands to configure the CA.

certutil -setreg ca\EncrpytionCSP\ProviderType 0x0

certutil -setreg ca\EncrpytionCSP\CNGEncryptionAlgorithm "AES"

certutil -setreg ca\EncrpytionCSP\SymmetricKeySize 192

## Performance Counters

This section describes the additions to Performance Monitor to examine counters that are related to the CA and its database. A management pack for Microsoft Operations Manager will be released Windows Server “Longhorn” post-Beta 2 that includes threshold definitions for those performance counters that are relevant for certificate services.

### Overview and Requirements

Windows Server “Longhorn” was developed with the goals of reliability and manageability. To support these goals from an administrative view, performance counters have been added for the CA, CA Connections, and CA database.

A Windows Server “Longhorn” administrator is able to create a granular performance profile about the behavior of the CA. On a stand-alone CA, each performance counter applies to the CA instance; on an enterprise CA, CA-related counters apply per template instance, where it makes sense. For example, on a stand-alone CA, you can monitor the failed requests per CA, while on an enterprise CA, you can watch failed requests for a specific certificate template.

Figure 22 illustrates how several performance counters can be added to a performance profile.



Figure : Performance Counters for Certificate Services

### Scenario

This section describes two sample scenarios where you can benefit from performance counters in certificate services.

#### Monitoring During Initial Certificate Enrollment

Contoso.com is a global enterprise company with about 50,000 Windows users. To deploy certificate-based services like IPsec or smart card logon, the company has decided to enroll computer and user certificates to all users and computers.

The administrators who have set up the CA are interested in statistical data during the certificate rollout. The main reason to monitor certificate enrollment closely is to verify the sizing of their CA infrastructure. Contoso has deployed two enterprise CAs to provide the greatest high availability. However, Contoso has no real experience of how much load is put on their CAs during initial certificate enrollment. The main question remains unanswered: "How will the CA behave if we assign the IPsec and smart card templates to the CAs?"

The PKI administrators of Contoso.com have found that performance counters for certificate services are the right instrument to monitor and ensure the health of their CAs.

#### Collecting Data to Create Health Reports to Back Up Service Level Agreements

The PKI administrators of Contoso have to satisfy internal service-level agreements (SLA) for certificate services. The SLAs define, for example, a minimum number of failed requests and a minimum request processing time to issue certificates.

The PKI administrators have found that with a Data Collector Set they are able to create reports formatted as HTML pages that will show all important indicators that prove the health-state of the PKI.

#### Configuration

Performance counters are installed together with a role service. If the CA is installed, performance counters for Certification Authority and Certificate Authority Connections are installed. Also, the certsrv instance is added to the Database, Database Instances, and Database TableClasses counters. The OCSP role service will add counters for OCSP Server and OCSP Server Connections.

Performance counters are created when a role service is installed and are removed from the system if a role service is uninstalled. That means that performance counters are already registered before a role service starts for the first time.

The following performance counter groups are relevant for certificate services.

* Certification Authority
* Certification Authority Connections
* Database
* Database Instances
* Database TableClasses

These performance counters are relevant if the OCSP responder role service is installed.

* OCSP Server
* OCSP Server Connections

You can watch the Certificate Server performance counters locally or remotely from a Windows Server Longhorn, Windows Vista, Windows Server 2003, or Windows XP computer. To access counter data on a remote computer, the remote computer must have the Remote Registry service enabled. For more developer-related information about performance counters, see the MSDN Web page at
<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/perfmon/base/performance_monitoring_reference.asp>

For ad-hoc analysis of the certificate server behavior, add counters in the Windows Server “Longhorn” Performance Diagnostic Console.

**To add counters**

1. Log on to the computer where you want to monitor the Certificate Server role.
2. On the Start menu, select Administrative Tools, and then click Performance Diagnostic Console.
3. Once the Performance Diagnostic Console is open, expand the Monitoring Tools container, and then select Performance Monitor.
4. On the Action menu, select Properties.
5. In the System Monitor Properties dialog box, select the Data tab.
6. Click Add.
7. In the list of available counters, select the ones that you are interested in, and then click Add after each selection.
8. To close the **Add Counters** and **System Monitor Properties** dialog boxes, click OK twice.

The selected counters appear in the Performance Monitor graph.

To monitor your certificate server role in a more sophisticated way, create a data collector set to group the performance counters that you are interested in. For more information about Data Collector Sets, see "Understanding Data Collector Sets" in the Windows Server “Longhorn” online Help.

### Troubleshooting

This section provides troubleshooting information for issues relating to configuring performance counters.

#### Performance Counters are not installed properly after re-installation of Certificate Service

The Windows Server “Longhorn” Beta 2 release still has a problem with performance counters if the Certificate Services role service is re-installed on a Windows Server “Longhorn” computer. Performance counters are not displayed correctly, or even do not appear in the list of available counters. The problem will be fixed in a later release of Windows Server Longhorn.

## Manual Certificate Enrollment

Certificate enrollment can be performed manually or with auto enrollment. If done manually, you have a choice of synchronous or asynchronous. The manual synchronous enrollment is usually performed with the Certificates MMC Snap-In; the asynchronous enrollment can be done by carrying out certreq.exe from a command line.

This section explains how to enforce discrete signatures while enrolling certificates asynchronously. Discrete signatures for synchronous or auto enrollment are controlled with certificates.

#### Configuring Support for the Discrete Signature Algorithm (PKCS#1 V2.1 signatures) for CNG

If you are creating a certificate request manually with the certreq.exe command-line tool and want to use the PKCS#1 V2.1 signature in the certificate request, you have to use the DiscreteSignatureAlgorithm parameter in the .inf file.

To use the new algorithms that are available in Windows Vista and Windows Server Longhorn, you can carry out the following command to list the key providers that are available.

certutil -v -csplist

Only the version of the certutil program available in Windows Vista or Windows Server “Longhorn” will provide all the information that you need to build an .inf file for certreq.exe: Provider Name, Provider Type, and the supported algorithms per provider.

A properly formatted .inf file for certreq.exe would look like the following sample.

[Version]

Signature= "$Windows NT$"

[NewRequest]

HashAlgorithm = sha256

KeyAlgorithm = ECDSA\_P521

ProviderName = "Microsoft Software Key Storage Provider"

DiscreteSignatureAlgorithm = TRUE

The following output will help you verify the use of a discrete signature in a certificate request. It shows part of a certificate request dump. The certificate request was generated to use sha256 as hash algorithm in combination with ECDSA\_P521 as key algorithm and carries a discrete signature. The dump was created with the certutil -dump [requestfilename] command.

Signature Algorithm:

 Algorithm ObjectId: 1.2.840.10045.4.3 ECDSA Specified (specifiedECDSA)

 Algorithm Parameters:

 30 0d 06 09 60 86 48 01 65 03 04 02 01 05 00

 2.16.840.1.101.3.4.2.1 NIST SHA-256 (sha256/sha512NoSign)

 05 00

The output shows that the Algorithm Parameters attribute has the information about the algorithm that was used to hash the certificate request.

The same request without a discrete signature does not have any information in the Algorithm Parameters attribute. The attribute is just set to NULL.

Signature Algorithm:

 Algorithm ObjectId: 1.2.840.10045.4.3.2 ECDSA SHA-256 (sha256ECDSA)

 Algorithm Parameters: NULL

In case you are not specifying the HashAlgorithm parameter, certreq.exe will take SHA1 as the default. The default behavior handling is documented in RFC 4055 under section "2.2 Mask Generation Functions". A certificate request with a discrete signature looks like the following extract from a certificate request dump.

Signature Algorithm:

 Algorithm ObjectId: 1.2.840.113549.1.1.10 RSA SSA PSS (RSASSA-PSS)

 Algorithm Parameters:

 30 00

The Algorithm Parameters attribute is set to 30 00 which translates to an empty sequence. Because an empty sequence translates to the default value, SHA1 is implied. The following example is the same as the previous request with the DiscreteSignatureAlgorithm set to FALSE.

Signature Algorithm:

 Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA

 Algorithm Parameters:

 05 00

In this case, the Algorithm Parameter has a 05 00 sequence, which translates to NULL. A discrete signature is not used so far.

# Windows Integration

This section covers improvements to the Windows Server “Longhorn” Active Directory Certificate Services that provide better integration with Windows itself. The following topics are covered.

* Enterprise PKI MMC Snap-In provides an overview about the CA certificates and CRLs in the Active Directory forest.
* Web Enrollment.
* Key Distribution Center (KDC) certificate modification.

## Enterprise PKI (PKIview)

### Overview and Requirements

In an enterprise with one or more enterprise CAs, it might be difficult to keep track of the distribution points of CA certificates, CRLs, and AIAs. It is not only important to maintain the distribution points properly, but it is also important to ensure that all these items are accessible and current.

The PKI Viewer MMC Snap-In provides an overview at a glance of all CA certificates, CRLs, and AIAs that are available in your Active Directory environment.

The Enterprise PKI MMC Snap-In has the following limitations in Windows Server “Longhorn” Beta 2.

* The PKI view tool is intended for Active Directory environments only. If you use it on a workgroup computer, you will not be able to monitor your PKI.
* OCSP is not yet supported.

### Scenario

Contoso.com has internally implemented several PKI hierarchies, and needs a collective way to view and assess the health of these hierarchies. The enterprise hierarchies implemented have been published in Active Directory. If the help desk receives calls from users who are having problems logging on to Active Directory with their smart cards, it is important to know if the problem is with the CA.

### Configuration

To open the PKI View MMC Snap-In in an Active Directory environment, open an empty MMC and add the Enterprise PKI Snap-In to the list of selected snap-ins.

The user interface of the PKI management snap-in follows basic MMC design principles. The interface consists of the MMC scope pane (the tree view on the left of the console), the results pane (the various views in the right pane of the console), and various dialog boxes. Figure 23 illustrates a healthy Enterprise PKI.



Figure : Enterprise PKI MMC Snap-In

If your PKI is not healthy, the tree view illustrated in Figure 24 will show you what is wrong with your PKI environment.



Figure : Unhealthy PKI Environment

* If a CA is evaluated for its health state, a question mark would appear over the CA icon.
* If a CA is in good working order, a green indicator appears over the CA icon.
* If a CA has a non-critical problem (for example, AIA information could not be retrieved), a yellow indicator appears over the CA icon. AIA info is critical according to the tool.
* If a CA has a critical error (for example, the certificate is expired or revoked), a red indicator appears over the CA icon.
* If a CA is offline, an “CA is offline” message appears in the result pane and a red cross appears with the CA icon.

With the PKI Enterprise MMC Snap-In open, you can granularly examine the hierarchy of the CA certificates in the scope pane (left). The scope pane is a tree representation of the enterprise PKI hierarchy derived from the certificates gathered from Active Directory and current user’s certificate stores. Each item in the scope pane represents a CA; subordinate CAs are child items. The tree is built by enumerating the CAs with the ICertConfig API. CAPI2 is used for chain building.

Once a particular CA is highlighted in the left pane, the expiration status of the CA certificate, whether the chain validates properly, the status and validity of the AIA store, and the status and validity of the CDP store for that CA are displayed on the right pane. If an error was present with the AIA or CDP stores, a message indicating the error would appear (for example, "Unable to access the container – Permission Denied" or "The certificate downloaded from this AIA location does not match the issuer key identifier in the CA certificate.").

The result pane (right) for the Enterprise PKI MMC Snap-In is always a list view except for offline leaf CAs where it shows that the CA is offline. If the root item is selected in the scope pane, the result view shows the enterprise root CAs. If a CA is selected in the scope pane, the result pane shows any subordinate CAs, the CA certificate, any CRL distribution points listed in the certificate, and any AIA locations listed in the certificate. The result pane contains three columns: Name, Status, and Location. The protocols supported for the AIA and CDP locations are: file://, HTTP://, and LDAP://. The AIA and CRL distribution point locations for the root and intermediate CAs are gathered from the subordinate CA certificates. For the issuing CAs, the locations are gathered from contacting the CA directly.

To retrieve the details of a specific item in the right pane, select the item and select the View Certificate, View AIA Certificate, or View CRL option on the Action menu.

By clicking the Enterprise PKI node in the left pane, you can Manage Templates (which opens the certtmpl.msc MMC Snap-In internally) or set Options to how the certificate status, CRL status, and delta CRL expiring status is displayed in the PKI View MMC Snap-In.

With the Manage AD containers action, you have an option to verify and take corrective actions on CA certificates or CRL stores.

**Important** Be careful when deleting certificates in those containers. Figure 25 shows the NT AuthCertificates container where CA11 and CA12 were installed multiple times in the same environment. If you are certain that you do not need some of the certificates in one of the containers, you can carefully remove them. If you notice that certificates or CRLs are missing, you can add them manually. However, when adding items manually, you should determine the reason that the item is missing. Under normal conditions, the CA will take care of publishing certificates and CRLs to the distribution point if the CA is configured correctly.



Figure : Managing Certificate Services Configuration Containers

The tabs in the dialog box (Figure 25) display the names of the containers under the refer to the CN=Public Key Services,CN=Services,CN=Configuration,DC=... hive in Active Directory.

### Troubleshooting

Chain validation errors are one of the most common reasons why certificate operations fail. If you experience chain verification errors with PKIview, you should consider CAPI2 logging support in Windows Vista or Windows Server “Longhorn” to find out what is causing the actual failure.

For general CLR troubleshooting, see the “Certificate Revocation and Status Checking” document at
<http://www.microsoft.com/technet/prodtechnol/winxppro/support/tshtcrl.mspx>

#### Enabling CAPI2 logging to troubleshoot chain validation errors

For detailed information about the Windows internal operations during chain validation, enable logging for the CAPI2 application log.

1. Log on with local administrator permissions to the computer where the failure occurs.
2. Click the **Start** menu. On the Administrative Tools menu, click Event Viewer.
3. In the left pane, expand the Application Logs container, expand Microsoft, expand Windows, and then expand the CAPI2 container. Select the Operational container.
4. On the Action menu, click Properties.
5. In the General tab, select the Enable logging check box, adjust the maximum log size and log maintenance according to your needs, and then click OK.

With CAPI2 logging turned on, all chain validation operations are logged in the event log: Application logs - Microsoft - Windows - CAPI2.

**To find out what goes wrong with chain validation**

1. Open the event log on the computer where the chain validation fails and make sure CAPI2 logging is enabled.
2. In **Event Viewer** (Figure 26), expand the following container structure in the left pane. Application logs - Microsoft - Windows - CAPI2 - Operational
3. In the right pane, select a log entry that has an Error level.
4. In the bottom window, click the Details tab, and then select the Friendly View.



Figure : Viewing the CAPI2Log with Event Viewer

1. In Figure 26, you can see that the Certificate Services service failed to check the revocation for a certificate. The thumbprint of the certificate is shown as fileRef attribute in the Certificate section. With this information, you can begin troubleshooting the actual issue. Successful chain verification would always have a Result value of 0 (NULL).

For more information about how to troubleshoot CRL verification, see the “Certificate Revocation and Status Checking” document at
<http://www.microsoft.com/technet/prodtechnol/winxppro/support/tshtcrl.mspx>

## Web Enrollment

This section describes what has changed regarding the Certificate Services Web Enrollment in Windows Server “Longhorn” Beta 2.

### Overview and Requirements

Certificate Web enrollment has been available since the release of Windows 2000. Before you set up Web enrollment in Windows Server Longhorn, you should be aware of the following changes.

* In Windows Server “Longhorn” Beta 2, Web enrollment support is localized for U.S. English and German. All other languages that are supported by Microsoft will be available in the final release of Windows Server Longhorn.
* Enrollment on behalf (also known as smart card enrollment station) was removed from Web enrollment in Windows Server “Longhorn” because Windows Vista supports enrollment on behalf natively. If you need to perform enrollment on behalf with a Windows Server “Longhorn” Web enrollment, you should use Windows Vista computers as enrollment stations. Alternatively, you can use a Windows Server 2003 server with Web enrollment installed and enroll certificates on behalf from there through a Windows Server “Longhorn” CA.
* The Xenroll component was removed from Windows Server Longhorn, since Xenroll is replaced by CertEnroll in Windows Vista and Windows Server Longhorn. You cannot download the Xenroll CAB file from a Windows Server “Longhorn” Web enrollment configuration. If you are enrolling certificates through the Windows Server “Longhorn” Web enrollment pages from a Windows XP, Windows Server 2003, or Windows 2000 computer, the Web enrollment pages will detect this and use the Xenroll.dll that was installed locally on the client.
* Only Microsoft Internet Explorer V6.x and above or Netscape V8.1 is supported to submit certificate requests to the Web enrollment pages. If other types of Web browsers are used, only pre-generated PKCS#10 requests can be submitted to Web enrollment support to enroll for certificates.
* To maintain the state of pending requests, cookies are used. Make sure that the browser you are using for certificate enrollment through Web pages has cookie support enabled. Also, make sure that cookies are not deleted from the system before pending certificates have been enrolled.
* V3 certificate templates are not supported with certificate Web enrollment.
* Users cannot request machine certificates because it would require running Internet Explorer with administration privileges.

### Scenario

Contoso.com has a number of Windows workstations that are not joined to an Active Directory domain. With Web enrollment support, it is also possible for those users to authenticate with their Active Directory domain credentials, and request and enroll certificates through the CA Web interface.

Users who work on non-Windows operating systems must generate PKCS#10 requests on their computer first. Then, they can log on to the Web enrollment pages with their Active Directory user account and submit the PKCS#10 request as a BLOB to the Web enrollment pages to enroll a certificate.

### Configuration

The configuration work that needs to be done for Web enrollment support involves adding the role service to the server role.

If the Web enrollment support is installed on the same computer as the CA, no additional configuration steps are required. When the Web enrollment role service and the CA are installed on different computers, you have to set the target CA as part of the Web enrollment installation.

Note that you can only use V1 and V2 templates with Web enrollment support. V3 certificate templates are not supported here.

After the Web enrollment role service is installed, a new Web site CertSrv is available through the IIS configuration. If you need to examine the Web site configuration, use the **Internet Information Services (IIS) Manager** and expand the **Web Sites - Default Web Site CertSrv** container.

For more information about the Certificate Services Web enrollment support, see the “Configuring and Troubleshooting Windows 2000 and Windows Server 2003 Certificate Services Web Enrollment” document at
(<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/webenroll.mspx>)

The general information in this document is currently valid for Windows Server Longhorn.

Beta 2 Information: In Windows Server “Longhorn” Beta 2, the file that is used by Web enrollment support to find the CA is mistakenly located in the language-specific directory such as %SYSTEMROOT%\system32\certsrv\[language]\certdat.inc. This file will become a global configuration file that defines the configuration for all language packs that are installed for Web enrollment. If you have multiple language packs installed on an IIS computer, all certdat.inc files in the language-specific subdirectories must be identical.

#### Installing Multiple Languages for Certificate Web Enrollment on a Single Server

Windows Server “Longhorn” supports multiple language support for CA Web Enrollment. Besides the default operating systems language, other optional language packs can be installed.

**To support multiple languages on your CA Web enrollment**

1. Log on with local administrator permissions to the computer where CA Web enrollment was installed as a role service.
2. On the Start menu, click Run, type lpksetup.exe, and then click OK.
3. In the wizard, click Install languages.
4. Enter the path of the language files. Language packs are part of the Windows Server “Longhorn” installation medium and are found in the languagepacks directory.



Figure : Adding a Language Pack to the Current Windows Language

1. Select the language that you want to install, and then click Next.
2. After reading the license terms, select I accept the license terms, click Next, and then click Install.
3. To close the installation wizard, click Exit.
4. Click the **Start** menu to open the Internet Information Services (IIS) Manager, and then click Administrative Tools. The Internet Information Services (IIS) Manager MMC Snap-In opens.
5. In the left pane, expand the Computer node, expand Web Sites, expand Default Web Site, and then select CertSrv.
6. In the center pane, select Redirect Rules.
7. In the right pane, click Basic Properties.
8. Remove en-US from the Physical path so that the pathname looks like %SYSTEMROOT%\system32\CertSrv, and then click OK.
9. Closethe Internet Information Services (IIS) Manager.
10. On a Windows Server “Longhorn” Beta 2 computer, you must also type the following commands at a command-line prompt to make the Web enrollment configuration file available in every language-specific directory. Carry out the following command to change to the CertSrv subdirectory.

cd %SYSTEMROOT%\system32\CertSrv

1. For every language that is installed on the computer, carry out the following command.

copy EN-US\certdat.inc {language-id}

For example:

copy EN-US\certdat.inc DE-DE

For a complete list of language identifiers, see
<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/intl/nls_238z.asp>

As described previously, to maintain multiple language support with Web enrollment support, it is important to change the physical path of the CertSrv virtual directory to enable other languages than the default language. Once the default physical path is modified, clients must add the language identifier to the URL to access the Web enrollment pages. To verify multiple language support, open Internet Explorer and type http://{hostname}/certsrv/{LangID}, such as <http://localhost/certsrv/de-de>.

#### Upgrading Web Enrollment Support from Windows Server 2003 to Windows Server Longhorn

Windows Vista clients cannot enroll using Web enrollment support from Windows Server 2003. To fix this problem, see the (soon-to-be released) knowledge Base article at
<http://support.microsoft.com/default.aspx?scid=kb;en-us;922706>

#### Installation of 64-Bit Web Enrollment on an IIS Computer that Runs 32-Bit Web Applications

If you have the 64-bit version of Windows installed on the computer that runs the IIS, you must not install any 32-bit Web applications, such as Microsoft Windows Server Update Services (WSUS), on that computer. Otherwise, the Web enrollment role service installation fails because IIS can only run in 64-bit mode or 32-bit mode.

### Troubleshooting

#### Server Error in 'Default Web Site/CertSrv' Application.*HTTP Error 404.0 - Not Found*

This error can have multiple causes.

If you have multiple language support installed on the Web enrollment computer, the following error message might occur.

Server Error in 'Default Web Site/CertSrv' Application.

HTTP Error 404.0 - Not Found

…

Physical Path: D:\Windows\system32\CertSrv\en-US\de-de

Make sure that you have configured the Physical Path correctly in the IIS configuration as described in the Installing Multiple Languages for Certificate Web Enrollment on a Single Server section.

If the CA is not accessible, the following error message might occur.

Server Error in 'Default Web Site/CertSrv' Application.

HTTP Error 404.0 - Not Found

Description: The resource you are looking for might have been removed, had its name changed, or is temporarily unavailable.

Verify whether the CA is operational. Use the certutil -ping command to verify whether the configuration string that is specified in the certdat.inc file is accessible.

#### The Web site cannot display the page

If you try to connect to a localized Web enrollment page and have also included the language URL, the error message “The website cannot display the page” may occur if you did not copy the certdat.inc file from the EN-US subdirectory to the language-specific directory. See the “Installing Multiple Languages for Certificate Web Enrollment on a Single Server” section to copy the configuration file.

This is a Windows Server “Longhorn” Beta 2–specific error and will be fixed in a future preliminary version of Windows Server Longhorn.

#### Removing the Certification Authority from a computer where Web enrollment is installed fails

If you have installed a CA together with Web enrollment on the same computer, and you need to uninstall the CA on that computer, the removal procedure will result in the following error.

Active Directory Certificate Server

The following role services will be removed:

Certification Authority

Active Directory Certificate Server: Removal failed

The following role services were removed:

Certification Authority

The following role services were unexpectedly affected by the removal:

Certificate Authority Web Enrollment (Removed)

This is a non-critical error and informs you that the CA was removed but the Web enrollment support is still installed. To ensure that your Web enrollment support remains operational, re-target it to a different CA in your Active Directory environment. To do this, modify the sServerConfig parameter in the certinc.dat configuration file in the %SYSTEMROOT%\system32\CertSrv directory. Replace the parameter value with a valid fully qualified Domain Name System (DNS) name of a still existing CA in Active Directory.

## KDC Certificate Modification

This section describes how clients are able to better verify domain controller certificates.

### Overview and Requirements

The Windows 2000 enterprise CA has introduced the Domain Controller certificate template that was used by domain controllers to perform smart card authentication and also to secure Active Directory eMail replication.

To make domain controller authentication independent from secure Active Directory eMail replication, the Domain Controller certificate template was split into two certificate templates. The Domain Controller Authentication certificate has superseded the Domain Controller certificate template. Domain controllers would enroll a Domain Controller Authentication certificate instead of the two-functional Domain Controller certificate.

The Windows Server “Longhorn” CA introduces a new certificate template called Kerberos Authentication. It replaces the existing Domain Controller Authentication certificate template because it is more secure.

When a domain-joined client computer performs a PKINIT with a server, the client needs to be able to verify that the other computer has a valid certificate and that it actually is also a Domain Controller. The domain controller and the Domain Controller Authentication certificate add the domain controller’s fully qualified domain name (FQDN) to the certificate. However, with this information, a client is not able to truly verify whether the machine is a valid domain controller because a client does not have an authoritative list of all valid domain controllers for a domain. Therefore, the Kerberos Authentication certificate template adds the domain name instead of the domain controller’s FQDN to the certificate.

To benefit from the more secure Kerberos Authentication certificate, strong KDC validation can be enforced for Windows Vista and Windows Server “Longhorn” computers. By default, strong KDC validation is turned off for backwards compatibility for Windows versions prior to Windows Vista. To enable strong KDC validation, set the following registry value as a DWORD to 2; to disable KDC validation, set the value to 0.

HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters\kdcvalidation

If strong KDC validation is enabled, the client will require the presence of the 1.3.6.1.5.2.3.5 OID in the extended key usage (EKU) and the matching domain name in the subject alternate name. For more information about the implementation of strong KDC validation, see section 3.2.4 at
<http://www.ietf.org/internet-drafts/draft-ietf-cat-kerberos-pk-init-34.txt>

A Windows Server “Longhorn” domain controller selects its certificate based on the following rules.

1. Is there a certificate in the domain controller’s Personal Computer Certificate store that was issued with the Kerberos Authentication certificate template (identified by object identifier (OID) not by template name) and carries the OID 1.3.6.1.5.2.3.5 (id-pkinit-kpKDC) in the EKU attribute? If this is the case, the certificate is used for PKINIT authentication.
2. Otherwise, the domain controller searches its Personal Computer Certificate store for a certificate that was issued by the Domain Controller Authentication certificate template and carries the OID 1.3.6.1.4.1.311.20.2.2 (id-ms-kp-sc-logon) in the EKU attribute. If such a certificate is found, the certificate is used for PKINIT authentication.
3. Otherwise, the domain controller will search its Personal Computer Certificate store for a certificate that was issued using the Domain Controller certificate template. If such a certificate is found, the certificate is used for PKINIT authentication.
4. Otherwise, PKINIT authentication is disabled on this domain controller.

### Scenario

Contoso.com has found it can benefit from the strong KDC validation by enabling the associated registry setting. The company is going to configure Windows Vista clients so that those clients will mutually authenticate only with domain controllers that have a Kerberos Authentication certificate template issued.

### Configuration

Special configuration steps are not required to enroll Domain Controller certificates if a Windows Server “Longhorn” CA is introduced in an Active Directory environment.

A Windows Server “Longhorn” issues Domain Controller certificates to Windows Server 2003 and Windows Server “Longhorn” domain controllers only with the Kerberos Authentication certificate template by default. For Windows 2000 Domain Controllers, the Domain Controller certificate template is still used.

Because certificate auto enrollment has been turned on in Group Policies, domain controllers will enroll for Kerberos Authentication certificates automatically.

For more information about configuring certificate auto enrollment, see the “Certificate Autoenrollment in Windows Server 2003” at
<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/autoenro.mspx>

### Differences in Domain Controller Certificate Templates

Domain Controller certificate templates have been available since the release of Windows 2000. However, certificate templates for domain controllers have been improved in every Windows Server release. The core functionality of smart card logon is not affected by these changes; however, the newer certificate templates provide greater flexibility and granularity than their predecessors. The following table illustrates the differences in Domain Controller certificate templates.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute | Windows 2000 | Windows Server 2003 | Windows Server 2003 | Windows Server Longhorn |
| Subject | CN={FQDN} | Empty | Empty | Empty |
| Certificate Template | DomainController | Directory Email Replication | Domain Controller Authentication | Kerberos Authentication |
| Enhanced Key Usage | Client Authentication (1.3.6.1.5.5.7.3.2)Server Authentication (1.3.6.1.5.5.7.3.1) | Directory Service Email Replication (1.3.6.1.4.1.311.21.19) | Client Authentication (1.3.6.1.5.5.7.3.2)Server Authentication (1.3.6.1.5.5.7.3.1)Smart Card Logon (1.3.6.1.4.1.311.20.2.2) | Client Authentication (1.3.6.1.5.5.7.3.2)Server Authentication (1.3.6.1.5.5.7.3.1)Smart Card Logon (1.3.6.1.4.1.311.20.2.2)KDC Authentication (1.3.6.1.5.2.3.5) |
| Subject Alternate Name | Other Name:1.3.6.1.4.1.311.25.1={GUID}DNS Name={FQDN} | Other Name:1.3.6.1.4.1.311.25.1={GUID}DNS Name={FQDN} | DNS Name={FQDN-hostname} | DNS Name={FQDN-domainname}DNS Name={NetBIOS-Domain-Name} |

### Configuring Domain Controller Certificate Templates in Mixed Environments

As explained in the “Default Certificate Templates in Windows Server 2003 and Windows Server Longhorn” section, the Domain Controller, Directory Email Replication, and Kerberos Authentication certificate templates are assigned by default to a CA once it is installed.

The following table illustrates which certificate template is used in a configuration where a domain controller and CA are installed on different versions of Windows.

|  |
| --- |
| Certification Authority |
|  | Windows 2000 | Windows Server 2003 | Windows Server Longhorn |
| Windows 2000 Domain Controller | Domain Controller | Domain Controller | Domain Controller |
| Windows Server 2003 Domain Controller | Domain Controller | * Domain Controller

or* Domain Controller Authentication
* Directory eMail Encryption
 | Kerberos Authentication |
| Windows Server “Longhorn” Domain Controller | Domain Controller  | * Domain Controller

or* Domain Controller Authentication
* Directory eMail Encryption
 | Kerberos Authentication |

The following describes the exact enrollment behavior shown in the previous table.

* A Windows 2000 domain controller will always enroll a Domain Controller certificate from any CA version because Automatic Certificate Request Service (ACRS) is used. Even if newer certificate template types are available on a Windows Server 2003 or Windows Server “Longhorn” CA, a Windows 2000 domain controller will always use the Domain Controller certificate template.
* A Windows Server 2003 domain controller will enroll a Domain Controller certificate template from a Windows 2000 CA because there is no other Domain Controller certificate template. If the Certificate Services administrator has not manually assigned the Domain Controller Authentication and Directory eMail Encryption certificate template to a Windows Server 2003 CA, Windows Server 2003 domain controllers still use the default Domain Controller certificate template. If the Domain Controller Authentication and Directory eMail Encryption certificate were assigned to a Windows Server 2003 CA, auto enrollment for the Domain Controller certificate template should have been disabled in the Group Policy settings (Computer Configuration - Windows Settings - Security Settings - Public Key Policies - Automatic Certificate Request Settings). Otherwise, a Windows Server 2003 domain controller will enroll for a domain controller, a Domain Controller Authentication, and Directory eMail Encryption certificate. The reason for this behavior is that the Domain Controller certificate template and the Domain Controller Authentication/Directory eMail Encryption certificate template use different enrollment mechanisms. If a Windows Server “Longhorn” CA is available, a Windows Server 2003 domain controller will enroll for a Kerberos Authentication certificate. The Kerberos Authentication certificate supersedes the Domain Controller Authentication certificate template. Therefore, a Windows Server 2003 domain controller will re-enroll for a new Kerberos Authentication certificate as soon as the Kerberos Authentication certificate template becomes available. Or, it will enroll just for a Kerberos Authentication certificate if a Domain Controller Authentication certificate template would also be available. The Kerberos Authentication certificate template is fully backwards compatible with the previous domain controller templates so that, for example, smart card logon with a Windows Server “Longhorn” domain controller could be performed with even a Windows 2000 Professional computer.
Note In Windows Server “Longhorn” Beta 2, the Domain Controller Authentication certificate is not yet superseded by the Kerberos Authentication certificate template. This change will be implemented before the release of Windows Server Longhorn.
* Regarding Domain Controller certificate enrollment, a Windows Server “Longhorn” domain controller will follow the same enrollment logic as a Windows Server 2003 domain controller.

To enable a more secure PKINIT processing during smart card logon on a computer running Windows Vista or a later Windows version, you should enroll your domain controller for Kerberos Authentication certificate templates if a Windows Server “Longhorn” CA is available. If you still have a Windows Server 2003 CA, you should make available Domain Controller Authentication and, if required, Directory eMail Certificate templates.

# Compliant with Standards

This section covers standards compliance improvements for the Windows Server “Longhorn” Active Directory Certificate Services. The following topics are covered.

* IDP CRL extension support
* OCSP support
* MSCEP support

## IDP CRL Extension Support

This section explains how to add an issuing distribution point (IDP) to CRLs that are published with the Hypertext Transfer Protocol (HTTP) or Lightweight Directory Access Protocol (LDAP).

### Overview and Requirements

To support X.509– and RFC 3280–compliance the Windows Server “Longhorn” CA supports the IDP extension in CRLs. The IDP extension is a critical extension and to non-Windows clients, the use of IDP extension in CRLs ensures that relying parties can determine the proper scope of a CRL when a CA certificate is renewed or re-keyed (renew with new key). It indicates whether the CRL covers revocation for end-entity certificates only, CA certificates only, attribute certificates only, or a limited set of reason codes.

Any Windows client that has installed the CRL verification engine that is available in the security hotfix MS05-11 ([www.microsoft.com/technet/security/Bulletin/MS05-011.mspx](http://www.microsoft.com/technet/security/Bulletin/MS05-011.mspx)) is able to handle IDP extensions.

IDP CRL extension support improves RFC 3280–compliance. The feature can be enabled or disabled by a CA manager using the CRL properties dialog box or the certutil program.

The IDP CRL extension is added for a non-Windows client, and it will point to the same URL as the CDP extension.

The IDP CRL Extension supports only HTTP and LDAP.

### Scenario

Contoso.com has a few non-Windows computers in its IT environment. To support both Windows and non-Windows clients that have different behaviors for path validation and revocation status checking, IDP CRL support is required. With IDP extension in CRLs, Contoso.com ensures that relying parties can determine the proper scope of a CRL when a CA is renewed or renewed with a new key.

### Configuration

**To configure IDP CRL extension support using the CRL Properties dialog box**

1. Log on to the computer where the CA is installed with CA manager permissions.
2. On the Start menu, select Administrative Tools, and then select Certification Authority.
3. Select the **Certification Authority** node. On the **Action** menu, click Properties.
4. Click the Extensions tab.
5. Select the CRL in the list box where you want to set the IDP CRL extension.
6. Mark the Include in the IDP extension of issued CRLs option, and then click Apply.
7. Repeat steps 5 and 6 if you want to set the extension for different CRL distribution points.
8. To finish the configuration, click OK.

**Or, to use the certutil program to manipulate the IDP extension for a CRL distribution point**

1. Log on to the computer where the CA is installed with CA manager permissions.
2. On the Start menu, click Run, and then type **cmd**.
3. At the command-line prompt, to display the current CRL distribution points including their properties, type the following command.
certutil -getreg ca\CRLPublicationURLs
4. Every CRL distribution point contains a number at the beginning of the line. These numbers represent the CRL distribution point properties. To enable the CRL extension for a CRL distribution point, add 128 (decimal) to the number at the beginning of the line. In the following example, you would have to change the number to 138 (decimal).
10:ldap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10
Since the certutil program is not able to change specific parts of a multi-valued registry key, you must set the complete key again. The following example sets the CRL distribution point property for the HTTP and LDAP distribution point:
certutil -setreg CA\CRLPublicationURLs "1:%WINDIR%\system32\CertSrv\CertEnroll\%3%8%9.crl\n130:http://www.contoso.com/pki/%3%8%9.crl\n138:LDAP:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10"

For more information about how to manipulate the CRL distribution point with the certutil program, see “Configure the CorporateRootCA CRL and AIA CRL Distribution Point from a Batch File” section at
<http://technet2.microsoft.com/WindowsServer/en/Library/091cda67-79ec-481d-8a96-03e0be7374ed1033.mspx>

Note To enable the CRL extension, you have to publish a new CRL. However, clients will download a new CRL only if their locally cached copy is going to expire. Thus, it might take some time until clients will recognize the configuration change. It is a good practice to set the IDP extension when a CRL is published for the first time.

## OCSP Support

Support for OCSP is covered in a separate document. For more information about OCSP, see
[www.microsoft.com/pki](http://www.microsoft.com/pki)

## MSCEP

Microsoft Simple Certificate Enrollment Protocol (MSCEP) is covered in a separate document. For more information about MSCEP, see
[www.microsoft.com/pki](http://www.microsoft.com/pki)