

Infrastructure Planning  
and Design

Active Directory® Certificate Services

Version 1.1

Published: June 2010

Updated: November 2011

For the latest information, please see [www.microsoft.com/ipd](http://www.microsoft.com/ipd)

Copyright © 2011 Microsoft Corporation. All rights reserved. Complying with the applicable copyright laws is your responsibility.  By using or providing feedback on this documentation, you agree to the license agreement below.

If you are using this documentation solely for non-commercial purposes internally within YOUR company or organization, then this documentation is licensed to you under the Creative Commons Attribution-NonCommercial License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc/2.5/> or send a letter to Creative Commons, 543 Howard Street, 5th Floor, San Francisco, California, 94105, USA.

This documentation is provided to you for informational purposes only, and is provided to you entirely "AS IS".  Your use of the documentation cannot be understood as substituting for customized service and information that might be developed by Microsoft Corporation for a particular user based upon that user’s particular environment. To the extent permitted by law, MICROSOFT MAKES NO WARRANTY OF ANY KIND, DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, AND ASSUMES NO LIABILITY TO YOU FOR ANY DAMAGES OF ANY TYPE IN CONNECTION WITH THESE MATERIALS OR ANY INTELLECTUAL PROPERTY IN THEM.

Microsoft may have patents, patent applications, trademarks, or other intellectual property rights covering subject matter within this documentation.  Except as provided in a separate agreement from Microsoft, your use of this document does not give you any license to these patents, trademarks or other intellectual property.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious.

Microsoft, Active Directory, Hyper-V, Outlook, SharePoint, Windows, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries and regions.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

You have no obligation to give Microsoft any suggestions, comments or other feedback ("Feedback") relating to the documentation. However, if you do provide any Feedback to Microsoft then you provide to Microsoft, without charge, the right to use, share and commercialize your Feedback in any way and for any purpose.  You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft software or service that includes the Feedback.  You will not give Feedback that is subject to a license that requires Microsoft to license its software or documentation to third parties because we include your Feedback in them.

Contents

[The Planning and Design Series Approach 1](#_Toc300222833)

[Introduction to the Active Directory Certificate Services Guide 2](#_Toc300222834)

[Step 1: Identify the Certificate Requirements 6](#_Toc300222835)

[Step 2: Design the Root Certification Authority 8](#_Toc300222836)

[Step 3: Design the Certification Authority Hierarchy 10](#_Toc300222837)

[Step 4: Design the Certification Authority Server Infrastructure 13](#_Toc300222838)

[Conclusion 16](#_Toc300222839)

[Appendix A: Job Aids 17](#_Toc300222840)

[Appendix B: Applications and Services That Use Certificates 19](#_Toc300222841)

[Appendix C: Public Root Certificates 23](#_Toc300222842)

[Appendix D: What’s New in Windows Server 2008 R2 24](#_Toc300222843)

[Appendix E: Certificate Revocation Methods 25](#_Toc300222844)

[Appendix F: IPD in Microsoft Operations Framework 4.0 26](#_Toc300222845)

[Appendix G: Active Directory Certificate Services in Microsoft Infrastructure Optimization 27](#_Toc300222846)

[Version History 28](#_Toc300222847)

[Acknowledgments 29](#_Toc300222848)

# 

# The Planning and Design Series Approach

This guide is one in a series of planning and design guides that clarify and streamline the planning and design process for Microsoft® infrastructure technologies.

Each guide in the series addresses a unique infrastructure technology or scenario. These guides include the following topics:

* Defining the technical decision flow (flow chart) through the planning process.
* Describing the decisions to be made and the commonly available options to consider in making the decisions.
* Relating the decisions and options to the business in terms of cost, complexity, and other characteristics.
* Framing the decision in terms of additional questions to the business to ensure a comprehensive understanding of the appropriate business landscape.

The guides in this series are intended to complement and augment the product documentation.

## Benefits of Using This Guide

Using this guide will help an organization to plan the best architecture for the business and to deliver the most cost-effective Active Directory® Certificate Services (AD CS) technology.

Benefits for Business Stakeholders/Decision Makers:

* Most cost-effective design solution for an implementation. Infrastructure Planning and Design (IPD) eliminates over-architecting and overspending by precisely matching the technology solution to the business needs.
* Alignment between the business and IT from the beginning of the design process to the end.

Benefits for Infrastructure Stakeholders/Decision Makers:

* Authoritative guidance. Microsoft is the best source for guidance about the design of Microsoft products.
* Business validation questions to ensure the solution meets the requirements of both business and infrastructure stakeholders.
* High integrity design criteria that includes product limitations.
* Fault-tolerant infrastructure, where necessary.
* Proportionate system and network availability to meet business requirements.
* Infrastructure that is sized appropriately to meet business requirements.

**Benefits for** Consultants or Partners:

* Rapid readiness for consulting engagements.
* Planning and design template to standardize design and peer reviews.
* A “leave-behind” for pre- and post-sales visits to customer sites.
* General classroom instruction/preparation.

Benefits for the Entire Organization:

Using this guide should result in a design that will be sized, configured, and appropriately placed to deliver a solution for achieving stated business requirements, while considering the performance, capacity, manageability, and fault tolerance of the system.

# Introduction to the Active Directory Certificate Services Guide

Active Directory Certificate Services (AD CS) provides a public key infrastructure (PKI) that can be used to distribute certificates from a trusted source to enable:

* Secure data transmission to a known recipient through encryption.
* Signing of code and documents that confirms who the sender is and that the data has not been tampered with in any way.

This guide, when used in conjunction with product documentation, will help companies confidently design an Active Directory Certificate Services infrastructure.

## Assumptions

To limit the scope of material in this guide, the following assumptions have been made:

* The decision to implement Active Directory Certificate Services has already been made.
* The design for Active Directory Domain Services (AD DS) has been completed. The design of an AD DS is covered in Infrastructure Planning and Design Guide for Active Directory Domain Services at <http://go.microsoft.com/fwlink/?LinkId=157704>.
* This design is for use in a production environment. It is expected that a test environment will also be created to mirror the production environment in configuration.
* The reader has familiarity with PKIs and AD DS. This guide does not attempt to educate the reader on the features and capabilities of Microsoft products. The product documentation covers that information.

## Active Directory Certificate Services Design Process

This guide addresses the critical design decisions faced by most organizations when implementing a PKI using AD CS in Windows Server® 2008 R2. Although the guide is written specifically for AD CS in Windows Server 2008 R2, much of the guide’s content is applicable to prior versions of Windows Server.

When an application, device, or user requires a certificate, the PKI of AD CS must provide the following functions:

* The certificate must be present on the machine where it’s needed.
* The machine, or device, where the certificate will be validated, must be able to confirm the authenticity of the certificate by building the trust chain, or “chaining up,” to its trusted root certification authority (CA).
* That machine or device must be able to check that the certificate has not been revoked.

This guide’s goal is to address the most common scenarios, decisions, activities, options, tasks, and outcomes that most organizations will encounter. It does not attempt to address every possible scenario or permutation of a scenario. Readers who think their environment is unique and not covered by the scenarios presented in this guide should consider hiring a design consultant to address their needs.

This guide addresses the following decisions and/or activities that need to occur in planning an AD CS infrastructure. The steps below represent the most critical design elements in a well-planned AD CS design:

* Step 1: Identify the Certificate Requirements
* Step 2: Design the Root Certification Authority
* Step 3: Design the Certification Authority Hierarchy
* Step 4: Design the Certification Authority Server Infrastructure

Some of these items represent decisions that must be made. Where this is the case, a corresponding list of common response options will be presented.

Other items in this list represent tasks that must be carried out. These types of items are addressed because their presence is significant in order to complete the infrastructure design.

Figure 1 provides a graphical overview of the steps in designing an AD CS infrastructure.

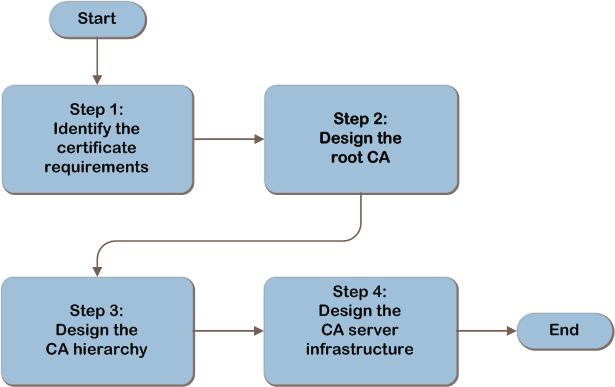


Figure 1. The AD CS infrastructure decision flow

Figure 2 illustrates the relationship between the components that can work together to deliver an AD CS solution.

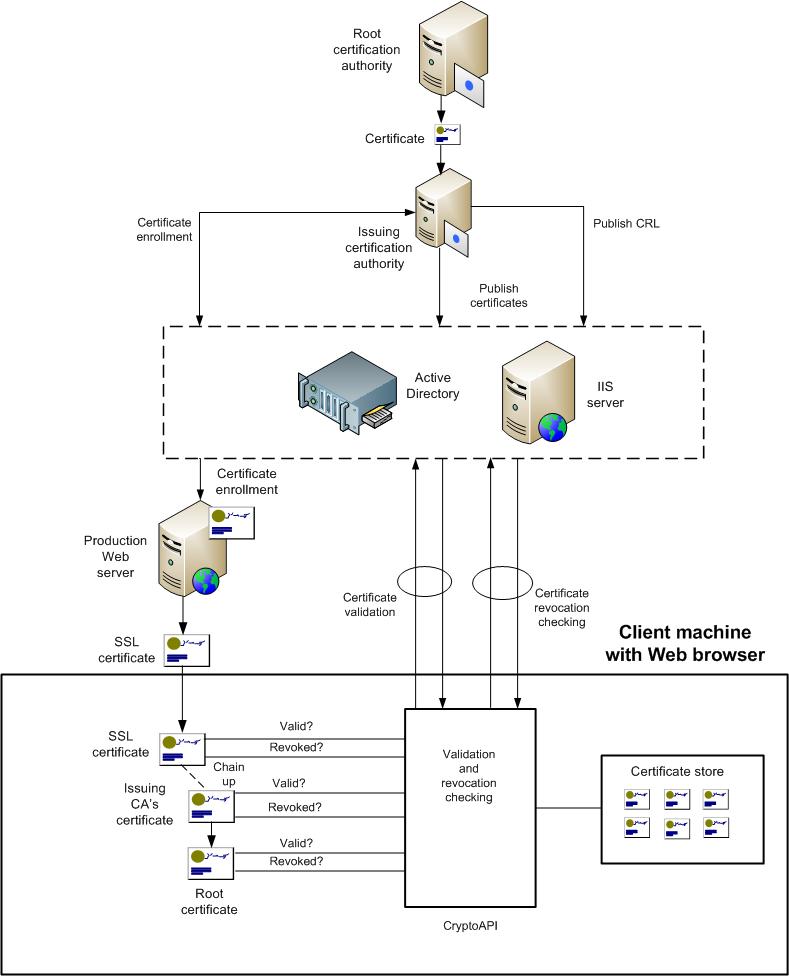


Figure 2. Example Active Directory Certificate Services architecture

## Applicable Scenarios

This guide addresses the planning and design decisions involved in creating a successful public key infrastructure using Active Directory Certificate Services. It addresses the following scenarios:

* Creation of a PKI using AD CS in Windows Server 2008 R2
* Integration of the PKI using AD CS with Active Directory Domain Services (AD DS) in Windows Server 2008 R2
* Support for any of the following applications and services:
* Secured HTTPS traffic
* Code signing
* Microsoft System Center Configuration Manager configured in native mode
* Encrypting File System (EFS) in Windows® operating systems
* Internet Protocol security (IPsec) protected network traffic
* DirectAccess feature in Windows 7 and Windows Server 2008 R2
* Smart cards
* Wireless local area networks (WLANs)
* Virtual private networks (VPNs)
* Secure/Multipurpose Internet Mail Extensions (S/MIME)
* Windows Phone and Windows Mobile devices connecting to Exchange Server infrastructures
* Mutual authentication of Exchange Server components

## Out of Scope

This document is designed to guide the architect through the process of designing the core implementation for AD CS. The scope of this IPD guide does not cover the following areas:

* Creation of PKIs using versions of Windows Server prior to Windows Server 2008 R2. However, much of the guide’s content is applicable to prior versions of Windows Server.
* Interoperation with third-party directory services.
* Support for applications and services running on operating systems other than Windows client and server operating systems.
* Certificate design and certificate template selection.
* Use of public root CAs, such as Verisign, Thawte, or GoDaddy.

# Step 1: Identify the Certificate Requirements

A user may access applications and services from multiple locations, such as different parts of the organization, public Wi-Fi hotspots, or from home. Certificate services must be available at any location from which the user or device will connect.

In this step, the project scope will be identified by defining which parts of the organization will be included in the project.

This information will be used in later steps to design and place the root CA as well as any additional infrastructure needed to enroll, validate, and perform revocation checking for certificates.

## Task 1: Identify Where Certificates Will Be Used

Start by defining which parts of the organization will be included in the project. For example, the project scope might include all enterprise servers and workstations, laptops used by mobile employees, workstations on a partner extranet that access corporate data for order fulfillment, or any client on the Internet, if information or services will be provided beyond the corporate firewall.

Once the project scope has been defined, determine where certificates will be used. For reference, a table listing examples of applications and services that require certificates is provided in Table B-1 “Applications and Services That Use Certificates” in Appendix B. That table provides a brief description of how the application or device uses certificates as well as the certificate requirements. In Table A-1 in Appendix A, record the following:

* Locations where certificates will be deployed. This will be used, along with the certificate enrollment method that is selected in Step 3, to design and place the issuing CAs.
* Locations where certificates will be validated, which includes chaining-up and revocation checking. If possible, for each location, estimate how many certificate validations are likely to occur during the course of a day and record that. This information will be used to design the CA hierarchy and the certificate revocation infrastructure.

The deployment location may be different from the location where the certificate is inspected. For example, an SSL certificate is deployed to a web server, but is validated from the browser client machine.

If certificate enrollment services are not available, this will affect the deployment of new application services or users. It will also prevent certificate renewals to existing services and the validation of certificates that are not already present in the CryptoAPI cache.

If certificate revocation services are not available, there is a risk that a compromised certificate will be used, which could create a security exposure.

For each application or service, review the impact of a potential failure in certificate services, and record in Table A-1 in Appendix A the fault-tolerance requirements for each application or service that will use certificate services. This will be used as input to the fault-tolerance design of the certificate services infrastructure in Step 4.

## Validating with the Business

Work with the business decision makers to ensure agreement and understanding of the certificate requirements. Ensure that the following questions are asked:

* Are there any additional legal, government, or regulatory requirements that may affect certificate usage? Local laws or industry regulations may impose limitations or controls on the certificate services design.
* Are the implications of using certificates for encryption fully understood? These implications might include:
* Encrypted traffic cannot be inspected for malicious content.
* Encryption and decryption will place an additional processing load on corporate servers.
* The use of certificates and encryption increases complexity in the environment.

## Step Summary

In this step, the project scope was identified by defining which parts of the organization will be included in the project. The fault-tolerance requirements for each application or service were identified as well. All of the data gathered in this step was recorded in Table A-1 in Appendix A.

*Additional Reading*

For more information about certificates and their uses see the following resources:

* Identify Your Certificate Requirements: <http://technet.microsoft.com/en-us/library/cc961518.aspx>
* Certificates: <http://technet.microsoft.com/en-us/library/cc700805.aspx>
* Malware and Signed Code: <http://blogs.technet.com/mmpc/archive/2008/11/06/malware-and-signed-code.aspx>
* PKI Enhancements in Windows 7 and Windows Server 2008 R2: <http://technet.microsoft.com/en-us/magazine/2009.05.pki.aspx?pr=blog>
* Komar, Brian. Windows Server 2008 PKI and Certificate Security. Microsoft Press ISBN-13:978-0-7356-2516-7, ISBN-10: 0-7356-2516-6. 2008
* “Windows PKI blog”: <http://blogs.technet.com/pki/archive/2007/08/19/windows-pki-documentation-reference.aspx>
* Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure: <http://technet.microsoft.com/en-us/library/cc772670(WS.10).aspx>

# Step 2: Design the Root Certification Authority

In the previous step, the project scope was decided and the fault-tolerance requirements of applications or services that will use certificates were identified. In this step, the number of root certification authorities (CAs), as well as the root CA type and location will be determined. This information will be used in later steps to design the CA hierarchy.

The root CA is the highest level in the certificate hierarchy in an organization. Start by planning for a single root CA, then add root CAs for any of the reasons listed in Task 1 below.

## Task 1: Determine the Number of Root CAs

The goal of this task is to determine whether more than one root CA is required, and then to decide where the root CA will be located. There is no technical reason to design more than one root CA, so plan for a single root CA. However, all applications and services that will use certificates must trust the root CA, so it may be necessary to design additional root CAs, for the following reasons:

* Business unit, division, or location that must be isolated and self-administering. This requirement may be based on:
* Laws, regulations, or other compliance standards.
* Restrictions that are part of the organization’s policy.

For example, a multinational organization may be required by law to have a separate root CA for each country or region where they have a location or business presence.

* Application or service that is required to administer certificates separately.   
  The owner of an application or service may require full control over all aspects of the application or service, including certificate security. In addition, some applications or services may have specific technical or compliance requirements mandating that certificates be administered separately.

Note that a single root CA can manage more than one Domain Name System (DNS) domain namespace. Namespaces are based on the DNS domain namespaces, so a single root CA can issue certificates for multiple DNS domain namespaces.

Although a DNS domain namespace typically has only one CA hierarchy, it is possible to have more than one—for example, a CA hierarchy for www.contoso.com and a different CA hierarchy for mail.contoso.com.

Record the number of root CAs as well as the reason for each in Table A-2 “Certificate Requirements to Design a Hierarchy of CAs” in Appendix A.

## Task 2: Determine the Root CA Type and Location

Perform this task for each root CA that was specified in the previous task.

The root CA can be deployed in one of the following ways:

* **Stand-alone root CA.** The CA is not integrated with AD DS. It operates in a workgroup and may be taken offline in order to maintain physical security.
* **Enterprise root CA.** Integrated with Active Directory Domain Services.
* **External root CA.** Operated by a third party beyond the organization’s firewall, it issues public root certificates. This is outside the scope of this guide but some information on it is provided in Appendix C.

Use the following table to decide which type of root CA will be used.

Table 1. Selecting the Root CA Type

|  |  |  |
| --- | --- | --- |
| Requirement | Stand-alone root CA | Enterprise root CA |
| Must be online | N | Y |
| Supports enterprise subordinate CA | Y | Y |
| Supports stand-alone subordinate CA | Y | N |
| Supports automated certificate management | Y – by using an enterprise subordinate CA | Y |

If an offline stand-alone root CA will be used, at least one online subordinate CA must be designed in Step 3. Add that to the certificate hierarchy requirements in Table A-2 so that it will be used as input to Step 4.

Record the CA type as well as the reason for the decision in Table A-2 in Appendix A.

## Step Summary

In this step, the number, type, and locations of root CAs were determined. The data gathered in this step was recorded in Table A-2 in Appendix A.

# Step 3: Design the Certification Authority Hierarchy

In the previous step, the root CA was designed. In this step, the minimal hierarchy of CAs will be designed under the root CA. This step must be repeated for each root CA that was designed in Step 2.

The following roles can exist in a CA hierarchy:

* **Root CA.** This is the highest level in the CA, and signs its own certificates.
* **Intermediate CA.** Subordinate to another CA in the hierarchy, it enables centralized policy administration across its subordinate CAs.
* **Issuing CA.** Subordinate to at least one other CA, it is the lowest level in the hierarchy.

All of these roles can perform the three certificate functions: certificate enrollment, validation, and revocation checking. And all of these functions can be combined on a single CA.

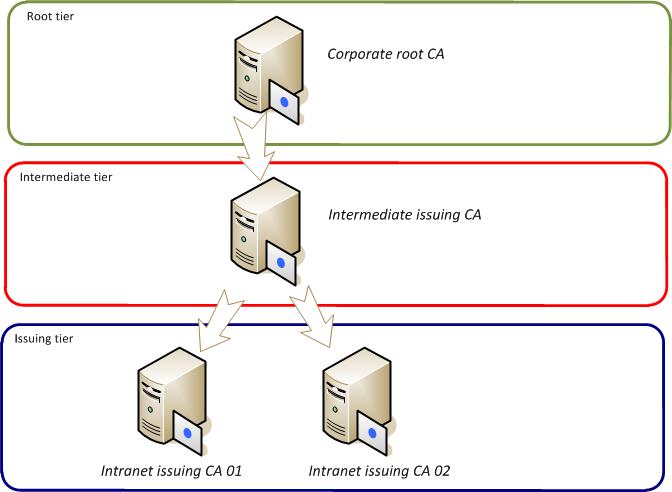


Figure 3. CA hierarchy

## Task 1: Determine the Number of Issuing CAs

Refer to Table A-2 to determine whether the root CA will be online or offline. If the root CA will be online, it can be used to provide certificate services. If the root CA will be offline, add one CA to the design. Record this in Table A-2 in Appendix A.

Issuing CAs can be added to the design as subordinates of the root CA. The three certificate services functions—certificate enrollment, validation, and revocation checking—can be performed by an issuing CA. The root CA can do this or, if an offline root is used, a subordinate CA can perform the functions.

Use the following process to determine whether CAs should be added to the hierarchy to meet the needs of the organization. Add CAs as necessary for the following reasons:

* **Regulatory requirements.** Regulations may require that a separate CA provide certificate services to a particular location or, for example, that web server certificates be validated by a separate issuing CA.
* **Political and organizational reasons.** A business unit within the organization may require its own issuing CA.
* **Low bandwidth locations.** If there are locations that are connected by low bandwidth links and if the load on the certificate service is expected to be high, design an issuing CA in each remote location.
* **Fault tolerance.** Refer to the fault-tolerance requirements that were recorded in Table A-1 in Appendix A. Fault tolerance for certificate services can be achieved by any, or all, of the following techniques:
* Design additional CAs. If this approach will be used, add CAs to the design to duplicate the function of the CAs that require fault tolerance. This technique cannot be used for a root CA because there can only be one active instance of a root CA in the PKI.
* Make each CA highly available. This approach will be covered in the next step when the servers are designed for high availability.

In Table A-2 in Appendix A, record the number of issuing CAs that will be required and where they will be placed. Also, record the fault-tolerance strategy for each issuing CA.

## Task 2: Determine the Number of Intermediate CAs

Intermediate CAs can optionally be added to the hierarchy design as additional layers that centralize policy administration across multiple subordinate CAs.

Designing a three-tier hierarchy with intermediate CAs increases the complexity of the environment. Requirements to implement different policies can be implemented in a two-tier hierarchy with additional issuing CAs. The Windows Server product group states that there are no scale limitations that require a middle tier, so avoid using intermediate CAs unless there is a compelling business reason for doing so.

If intermediate CAs will be used, determine the number that will be required in order to meet the organization’s needs, and then refer to the fault-tolerance requirements that were recorded in Table A-2 in Appendix A. Fault tolerance for certificate services can be achieved by any, or all, of the following techniques:

* Design additional intermediate CAs. If this approach will be used, add CAs to the design to duplicate the function of the CAs that require fault tolerance.
* Make each intermediate CA fault tolerant. This approach will be covered in the next step when the servers are designed for high availability.

Record the location, purpose, and fault-tolerance strategy for each intermediate CA, along with the layer in which it will be placed, in Table A-2 in Appendix A.

## Step Summary

In this step, the minimum hierarchy of CAs that will meet the needs of the organization was designed. The design decisions made in this step were recorded in Table A-2 in Appendix A.

## Additional Reading

* Types of certification authorities: <http://technet.microsoft.com/en-us/library/cc740257(WS.10).aspx>
* Enterprise certification authorities: <http://technet.microsoft.com/en-us/library/cc776874(WS.10).aspx>
* Stand-alone certification authorities: <http://technet.microsoft.com/en-us/library/cc780501(WS.10).aspx>

# Step 4: Design the Certification Authority Server Infrastructure

In the previous step, the CA hierarchy was designed. In this step, the servers that will be used to deliver certificate services will be designed for each CA in the hierarchy. If certificate services will be provided over HTTPS; the IIS servers will be designed. In each case, the servers will be designed to provide the required performance and fault tolerance.

Any of the CA roles can be run on either a physical or a virtualized server.

Perform this step for each CA, including an online root CA.

## Task 1: Design the Certificate Services Roles

The certificate enrollment, validation and revocation services can be provided using the protocols in Table 2.

Table 2. Certificate Services Protocols

|  |  |  |  |
| --- | --- | --- | --- |
| Service | HTTP/S | AD DS | OCSP |
| Enrollment | Y | Y | N |
| Validation | Y | Y | N |
| Revocation | Y | Y | Y |

For each location, decide which protocol will be used for each of the services, and record that in Table A-2. Then use this information to design and place the certificate services roles to meet the needs of all locations, using as few servers as possible.

For the first location, refer to services required in that location, map those to the protocol(s) that will be used to deliver the services, and then decide where the server(s) will be placed. Repeat this process for each location, adjusting as necessary the placement of the servers so that they can best meet the needs of the locations, again using as few servers as possible. When performing this for each location, aim to share roles on the same server unless there is a political reason to separate them. There is no technical reason why certificate enrollment, validation, and revocation services cannot be provided from the same server.

Record the placement of the CA servers and IIS servers in Table A-2.

## Task 2: Design the CA Servers

Perform this task for each CA server that was placed in the previous task and recorded in Table A-2 in Appendix A.

The Certificate Services product group recommends that each CA should run on a dedicated server and that sharing the CA with a domain controller should be strongly discouraged. So begin the design with a single server, following the recommended server configuration listed at [www.microsoft.com/windowsserver2008/en/us/system-requirements.aspx](http://www.microsoft.com/windowsserver2008/en/us/system-requirements.aspx).

Benchmark information is available at <http://blogs.technet.com/wincat/archive/2009/08/10/scale-testing-the-world-s-largest-pki-all-running-on-ws08r2-and-hyper-v.aspx>.

Use this along with the guidance from the product group for Windows Server 2003 at <http://technet2.microsoft.com/WindowsServer/en/library/61b3334a-eb6d-4d7d-b122-ca0c6ab18f5f1033.mspx>. The AD CS product group states that this guidance is applicable to Windows Server 2008 R2.

Plan the server’s storage based on the number of certificates that will be enrolled and the amount of certificate data. The Windows Server product documentation states that for a single certificate, 64 KB of disk space should be sufficient, which includes the certificate request and, if used, a recovery key.

Refer to the fault-tolerance requirements for certificate services that were determined in Step 3. If fault tolerance is required, this can be achieved in two ways:

* Additional issuing CAs can be added to the design and placed behind a load balancer. In the event that one of the servers fails, requests can be redirected to the other servers. Note that this approach cannot be used for the root CA since there can only be one instance of the root CA.
* The CA server can be run in a failover cluster, and this is documented at <http://technet.microsoft.com/en-us/library/cc742424(WS.10).aspx>. However, note that this cluster is limited to two servers. Refer to <http://technet.microsoft.com/en-us/library/cc742517(WS.10).aspx> for information on setting up CA servers in a cluster.

Record the configuration, location, and fault-tolerance approach for each CA server in Table A-2 in Appendix A.

Note   If a hardware security module (HSM) will be used to generate and store the private key, refer to the HSM vendor’s documentation to design the HSM specific architecture.

## Task 3: Design the IIS Servers

Refer to Table A-3 where the output of Step 4 Task 1 was recorded. If Internet Information Services (IIS) servers will be included in the design, continue with this task; otherwise skip to the next task. IIS servers may be used to perform four different certificate services functions, and all of these can be implemented on the same server. They can be run on the CA server, or on a separate server. If the IIS server will be placed in a perimeter network, also known as DMZ, to provide services on the Internet, this will normally require role separation from the CA server, which is inside the corporate firewall.

Refer to Table A-2 in Appendix A to determine where the IIS servers will be required and in which roles. Then use the information in the following table to design the minimum number of IIS servers that will perform the required roles.

Table 3. Active Directory Certificate Services IIS Roles

|  |  |  |
| --- | --- | --- |
| IIS role | Protocol | IIS failover clustering |
| Certificate enrollment | HTTPS | Y |
| Certificate validation | HTTP | Y |
| CRL publication | HTTP | Y |
| Online responder for OCSP | HTTP | Not supported. Use load-balanced array or hardware load balancer. |

For each location where IIS servers will be used, refer to Steps 1 through 6 of Infrastructure Planning and Design Guide for *Internet Information Services 7.0 and Internet Information Services 7.5* at <http://go.microsoft.com/fwlink/?LinkId=157703> to design the servers using the following inputs:

* In Step 1 of the IIS guide, the site list will be the list of sites where IIS services are required.
* In Step 2 of the IIS guide, the application inventory will include the certificate services from the above table.

Record in Table A-2 in Appendix A the number and locations of the IIS servers and the roles that each will perform.

## Step Summary

In this step, the root CA server, issuing CA servers, and the intermediate CA servers were designed. In addition, the IIS servers were designed and placed. The data gathered in this step was recorded in Table A-2 in Appendix A.

## Additional Reading

* Windows Server 2008 R2 with SP1 System Requirements: <http://www.microsoft.com/windowsserver2008/en/us/system-requirements.aspx>
* “Scale testing the world’s largest PKI… all running on WS08R2 and Hyper-V®”: <http://blogs.technet.com/wincat/archive/2009/08/10/scale-testing-the-world-s-largest-pki-all-running-on-ws08r2-and-hyper-v.aspx>
* Evaluating CA Capacity, Performance, and Scalability: <http://technet.microsoft.com/en-us/library/cc778985(WS.10).aspx>
* Overview of CA Clustering: <http://technet.microsoft.com/en-us/library/cc742424(WS.10).aspx>
* Certification Authority Clustering Configuration and Troubleshooting Guide: <http://technet.microsoft.com/en-us/library/cc742517(WS.10).aspx>
* “PKI Enhancements in Windows 7 and Windows Server 2008 R2”: <http://technet.microsoft.com/en-us/magazine/2009.05.pki.aspx?pr=blog>
* “Implementing an OCSP responder: Part I - Introducing OCSP”: <http://blogs.technet.com/askds/archive/2009/06/24/implementing-an-ocsp-responder-part-i-introducing-ocsp.aspx>
* Certificate Revocation and Status Checking: <http://technet.microsoft.com/en-us/library/bb457027.aspx>
* “Designing and Implementing a PKI: Part I Design and Planning”: <http://blogs.technet.com/askds/archive/2009/09/01/designing-and-implementing-a-pki-part-i-design-and-planning.aspx>

# Conclusion

This guide has focused on summarizing the critical design decisions, activities, and tasks required to successfully design a public key infrastructure using Active Directory Certificate Services in Windows Server 2008 R2.

Once the certificate requirements were identified, they were used to design the root CAs. Then for each root CA, the CA hierarchy was determined, and finally the CA servers, IIS servers, and file servers were designed.

The guide has addressed the technical aspects, service characteristics, and business requirements needed to complete a comprehensive review of the decision-making process. When used in conjunction with product documentation, this guide can help organizations confidently plan implementation of public key infrastructures using Active Directory Certificate Services.

# Appendix A: Job Aids

The tables below are provided to assist the designer in planning a successful Active Directory Certificate Services infrastructure.

**Step 1**

Table A-1. Project Scope

|  |  |
| --- | --- |
| Project Scope | Requirements |
| **User population** |  |
| **Computers** |  |
| **Certificate locations** |  |
| **Number of certificates** |  |
| **Locations where certificates will be inspected** |  |
| **Fault-tolerance requirements for certificate services for locations** |  |
| **How certificates will be made available for validation** |  |
| **Certificate revocation** |  |

**Steps 2, 3, and 4**

Table A-2. Certificate Requirements to Design a Hierarchy of CAs

|  |  |
| --- | --- |
| Certificate requirements  for CA design hierarchy | Requirements |
| **Number of  root CAs** |  |
| **Location of each root CA** |  |
| Reason for  stand-alone or enterprise CA |  |
| Offline root CAs |  |
| Number of issuing CAs |  |
| Certificate enrollment requirements |  |
| Certificate validation requirements | *Active Directory, Web* |
| Certificate revocation requirements | *CRL, OCSP* |
| Number of intermediate CAs |  |
| Location of each intermediate CA |  |
| Reason for intermediate CA |  |
| Layer placement of intermediate CA |  |
| Fault-tolerance approach for each CA |  |
| Location of web servers |  |
| Server configuration for each root CA server |  |
| Location of each root CA server |  |
| IIS role |  |

# Appendix B: Applications and Services That Use Certificates

The following table is for reference and lists examples of applications and services that require certificates.

Table B-1. Applications and Services That Use Certificates

| Application or service | Usage | Certificate requirements |
| --- | --- | --- |
| Encrypt HTTPS traffic using Secure Sockets Layer (SSL).  Validate the identity of the web server. | Used by the web client to encrypt traffic between it and the web server.  Used by the web client to validate the identity of the web server in order to prevent a malicious server from masquerading. | Certificate on each web server.  CA chain must be accessible from all potential web clients so that the web client can validate the certificate of the root CA and any intermediate CAs. |
| Manage encrypted HTTPS traffic using ISA server and web publishing. | Used to decrypt and inspect traffic, then pass it to the web server using HTTP. | Certificate on the ISA server.  CA chain must be accessible from all potential web clients. |
| Used to decrypt and inspect traffic, then re-encrypt and pass it to the web server using HTTPS/SSL. | Certificate on the ISA server.  Certificate on the web server.  CA chain must be accessible from all potential web clients. |
| Authenticate the SSL client. | Prove the identity of the client when it connects to the web server. The use of this certificate is optional in SSL. | Certificate on all potential web clients. Private key on the web client and public key available to the web servers. |
| Code and document signing. | Prove the identity of the distributor of that code or document, and prove that the code or document has not been changed since it was signed. | Certificate at the point of code or document signature.  All potential recipients must have access to the chain up to the root CA. |
| System Center Configuration Manager 2007, running in native mode. | With Configuration Manager, a site can be configured in native mode in order to secure communication between the site server, site roles, and the clients. | Certificate on the site server and on all clients, to verify downloaded policies.  Web server certificates on the following site system roles, for SSL communications:   * Management point * Proxy management point * Distribution point * Software update point * State migration point * Client authentication certificates on all Configuration Manager clients |
| Encrypting File System (EFS) | EFS is a Windows encryption technology used to store encrypted files on NTFS file system volumes. Encrypted files cannot be used unless the user has access to the keys required to decrypt the information. | Certificate on the encrypting machine.  Certificate on the decrypting machine.  Recovery key on a domain controller. |
| Virtual Private Networks (VPNs) | L2TP (IPsec) and SSTP VPNs can use certificates to encrypt traffic that is sent through the VPN connection.  PPTP VPNs and SSTP VPNs can use certificates to implement EAP-TLS authentication. | If PPTP VPN uses EAP-TLS for authentication, a certificate is required on each VPN server. CA chain must be accessible from all potential clients.  L2TP (IPsec) VPN requires certificates at each VPN server and on all potential clients.  SSTP VPN requires certificate on each SSTP server.  CA chain must be accessible from all potential clients.  If SSTP VPN uses EAP-TLS for authentication, a certificate is required on each server. CA chain must be accessible from all potential clients. |
| IPsec | IPsec uses certificates to mutually authenticate two endpoints, and then encrypt and sign all communications between them. | Requires a certificate at each computer that will use IPsec. |
| DirectAccess | DirectAccess is introduced in the Windows 7 and Windows Server 2008 R2 operating systems. DirectAccess allows remote users to securely access enterprise shares, websites, and applications without connecting to a VPN. | DirectAccess uses IPsec, so certificates are required on each DirectAccess server and on all DirectAccess clients.  If IP-HTTPS is used, an SSL certificate is required on the DirectAccess server.  A certificate is required on each network location server, for HTTPS/SSL communication with intranet clients. |

| Application or service | Usage | Certificate requirements |
| --- | --- | --- |
| Smart cards | Smart cards may be used to implement multi-factor authentication. | Certificate on each smart card.  Every location from which the smart card may be used must be able to chain up to the root CA. |
| WLANs | WLANs can be secured using a wireless security infrastructure built with 802.1x. Certificates can be used for mutual authentication and encryption of traffic. | For EAP-TLS authentication: certificate on each client and certificate on the RADIUS server. Certificate is NOT required on the WAP server.  For PEAP authentication: a certificate is required on each RADIUS server. |
| S/MIME | S/MIME is used as a standard for public key encryption and signing of email encapsulated in MIME. S/MIME is natively supported in Microsoft Office Outlook® and Outlook Web Access in Exchange Server with the S/MIME control.  SSL can be used to encrypt email traffic as well as to validate the identity of the email server. | For S/MIME signing: certificate on the sender.  For S/MIME encryption: certificate on the recipient.  For SSL encryption: certificate on each mail server. |
| Windows Mobile devices | Windows Mobile devices use certificates for encryption of traffic and optionally for authentication of the Exchange ActiveSync feature.  For more information about the certificate requirements for Windows Mobile, see “Choosing an Authentication Method for Your Exchange ActiveSync Server” at <http://technet.microsoft.com/en-us/library/bb232023(EXCHG.80).aspx>. | For (optional) HTTPS/SSL encryption and authentication of the server: certificate on the server.  To optionally authenticate the client, a certificate on each client that may connect. |
| Exchange Server 2007 | Computers running Exchange Server use certificates for authentication and encryption of traffic between servers and between servers and clients.  For more information on the certificate requirements for Exchange Server, see “Certificate Use in Exchange Server” at <http://technet.microsoft.com/en-us/library/bb851505.aspx>. | For SMTP encryption and authentication: certificates on the Hub Transport servers and on Edge Transport servers.  For EdgeSync LDAP encryption: certificate on the Edge Transport server.  For POP3 and IMAP authentication: certificate on the Client Access server.  For Unified Messaging: certificate on the Hub Transport server, the UM IP Gateway and Communications Server 2007.  For Autodiscover: certificate on the Client Access server.  For Client Access HTTP clients: certificate on the Client Access server. |
| Unified Access Gateway (UAG) | The UAG server acts as the front end for Exchange, SharePoint®, Dynamics CRM, DirectAccess, and others. It communicates with the client workstation on behalf of the server application. | Certificate on the UAG server, replacing the client communications certificate on the application’s server. |

# Appendix C: Public Root Certificates

Organizations can select to use public or private root certificates. Public root certificates are typically purchased from and are issued by external CAs and are natively trusted by Windows operating systems. Private root certificates are typically issued by internal CAs and must be added to the list of trusted root CAs in Windows operating systems.

An organization can select to use only public root certificates, only private root certificates, or a combination of both public and private root certificates.

Use public root certificates when:

* Users and devices that access the applications are located outside the organization’s intranet**.** When users and devices are not directly connected to the organization’s intranet, it is more complicated to add a certificate for a trusted root CA on the intranet to the device. For external users, having a trusted root certificate that is already in the list of trusted root CAs on the devices makes the applications and services more readily accessible.
* Minimal control and management is available for the users and devices that access the applications**.** It is more complicated to add a certificate for a trusted root CA for unmanaged users and devices. For example, if users and their devices are unmanaged, automated methods for adding the certificate to the local certificate store on the device may be complicated and increase support costs and effort.
* It is highly desirable to minimize any configuration or complexity on the part of the users**.** If the users are not part of the organization, then it may be desirable to not require any manual effort on their part. For example, if users access a commerce website, requiring them to add a certificate for a trusted root CA may reduce business or prevent them from accessing the site altogether.

Select private root certificates when:

* Users and devices that access the applications are located inside the organization’s intranet**.** When users and their devices are directly connected to the organization’s intranet, it is easier to deploy the certificates to the devices. If the organization has the appropriate infrastructure, deploying the certificates can be highly-automated.
* A high-degree of control and management is available for the users and devices that access the applications**.** Users that are part of the organization can be required to install the certificates by the organization’s policy. And if the devices are highly managed, deploying the certificate can be included as a normal part of the day-to-day management process.

# Appendix D: What’s New in Windows Server 2008 R2

Active Directory Certificate Services in the Windows Server 2008 R2 operating system includes many new features that help improve public key infrastructure and certificate manageability, supportability, and performance, including the following:

* Uses Certificate Enrollment Web Service to support certificate enrollment using HTTP.
* Uses Certificate Enrollment Web Policy Service to support certificate enrollment using HTTP.
* Supports certificate auto-enrollment across Active Directory forests. Prior to Windows Server 2008 R2, certificate auto-enrollment was only supported within a single forest.
* Provides improved support for high-volume certification authorities.

For more details on the changes, see “PKI Enhancements in Windows 7 and Windows Server 2008 R2” at <http://technet.microsoft.com/en-us/magazine/2009.05.pki.aspx?pr=blog>.

If AD CS will be deployed in a Windows 2000 Server or Windows Server 2003 Active Directory environment, domain controllers do not need to be upgraded to Windows Server 2008. Likewise, neither the domain functional level, nor the forest functional level, needs to be changed.

# Appendix E: Certificate Revocation Methods

When a certificate is used, its validity is first confirmed, and then a check is made to ensure that the certificate has not been revoked. There are three ways in which the revocation check can be performed:

* Base Certificate Revocation List (CRL). The CA publishes a list of the serial numbers of revoked certificates on a regular basis. The list can be published in AD DS, using an HTTP URL or in a network shared folder specified in a UNC path. When a certificate’s revocation status is checked, the entire CRL is downloaded and the check is performed locally on the machine where the certificate is being used. The CRL is then stored in the CryptoAPI cache, and future calls will be made against the cached copy, unless it is time-expired or replaced by an updated CRL.
* Delta Certificate Revocation List (CRL). This is a list of updates to the base CRL. It will typically be much smaller than the base CRL, and it will be re-issued more frequently than the base CRL.

A revocation test requires that both the delta CRL and the base CRL be available. When a certificate’s revocation status is checked using the delta CRL, that CRL is first downloaded and the check is performed locally on the machine where the certificate is being used. The delta CRL is then stored in the CryptoAPI cache and future calls will be made against the cached copy, unless it is time-expired or replaced by an updated CRL.

* Online Certificate Status Protocol (OCSP). This uses an Online Responder service that dynamically queries either the CA database, or the published base and delta CRLs. A response is returned to the client indicating the revocation status of the certificate. It will normally provide more authoritative revocation information than a CRL, which is in the CryptoAPI cache and, therefore, may be out-of-date. In addition, it creates a much smaller network load than distribution of the entire CRL.

This capability is new in Windows Server 2008 and is supported by the following clients:

* Windows Vista®
* Windows 7
* Windows Server 2008
* Windows Server 2008 R2

# Appendix F: IPD in Microsoft Operations Framework 4.0

Microsoft Operations Framework (MOF) offers integrated best practices, principles, and activities to assist an organization in achieving reliable solutions and services. MOF provides guidance to help individuals and organizations create, operate, and support technology services, while helping to ensure the investment in technology delivers expected business value at an acceptable level of risk. MOF’s question-based guidance helps to determine what is needed for an organization now, as well as providing activities that will keep the organization running efficiently and effectively in the future.

Use MOF with IPD guides to ensure that people and process considerations are addressed when changes to an organization’s technology services are being planned.

* Use the Plan Phase to maintain focus on meeting business needs, consider business requirements and constraints, and align business strategy with the technology strategy. IPD helps to define an architecture that delivers the right solution as determined in the Plan Phase.
* Use the Deliver Phase to build solutions and deploy updated technology. In this phase, IPD helps IT pros design their technology infrastructures.
* Use the Operate Phase to plan for operations, service monitoring and control, as well as troubleshooting. The appropriate infrastructure, built with the help of IPD guides, can increase the efficiency and effectiveness of operating activities.
* Use the Manage Layer to work effectively and efficiently to make decisions that are in compliance with management objectives. The full value of sound architectural practices embodied in IPD will help deliver value to the top levels of a business.



Figure F-1. The architecture of Microsoft Operations Framework (MOF) 4.0

# Appendix G: Active Directory Certificate Services in Microsoft Infrastructure Optimization

The Infrastructure Optimization (IO) Model at Microsoft groups IT processes and technologies across a continuum of organizational maturity. (For more information, see [www.microsoft.com/infrastructure](http://www.microsoft.com/infrastructure).) The model was developed by industry analysts, the Massachusetts Institute of Technology (MIT) Center for Information Systems Research (CISR), and Microsoft's own experiences with its enterprise customers. A key goal for Microsoft in creating the Infrastructure Optimization Model was to develop a simple way to use a maturity framework that is flexible and can easily be applied as the benchmark for technical capability and business value.

IO is structured around three information technology models: Core Infrastructure Optimization, Application Platform Optimization, and Business Productivity Infrastructure Optimization. According to the Core Infrastructure Optimization Model, having a well-planned Active Directory Certificate Services infrastructure will help move an organization to the Dynamic level. Active Directory Certificate Services gives the administrator control over certificate enrollment, certificate revocation, and other public key infrastructure services needed by the applications and services running in the organization. On the path to the Dynamic level, organizations can use Active Directory Certificate Services to automatically enroll and renew certificates required for applications and services, such as System Center Configuration Manager or DirectAccess in Windows 7.

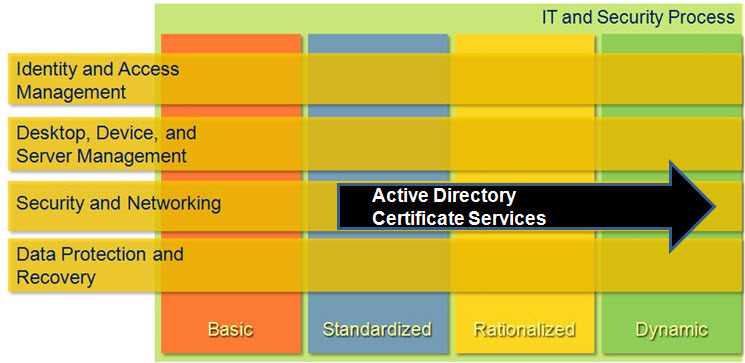


Figure G-1. Mapping of Active Directory Certificate Services technology into the Core Infrastructure Optimization Model

# Version History

|  |  |  |
| --- | --- | --- |
| **Version** | **Description** | **Date** |
| 1.1 | Minor updates for formatting consistency. | November 2011 |
| 1.0 | First release. | June 2010 |

# 

# Acknowledgments

The Solution Accelerators–Management and Infrastructure (SA-MI) team acknowledges and thanks the people who produced the *Infrastructure Planning and Design Guide for Active Directory Certificate Services*. The following people were either directly responsible for or made a substantial contribution to the writing, development, and testing of this guide.

**Contributors:**

* Jude Chosnyk – *GrandMasters*
* Joe Coulombe – *Microsoft*
* Michael Kaczmarek – *Microsoft*
* Douglas Steen – *Xtreme Consulting*
* Fergus Stewart – *Microsoft*
* Melissa Stowe– *Microsoft*
* Henry Webb *– Microsoft*

**Reviewers:**

* Eelco de Boer – Capgemini
* Claus Jespersen– Microsoft
* John Morello – Microsoft
* Florian Schneider – Microsoft

**Editor:**

* Laurie Dunham – *Xtreme Consulting*
* Pat Rytkonen – *Volt Technical Services*

## Feedback

Please direct questions and comments about this guide to [ipdfdbk@microsoft.com](mailto:ipdfdbk@microsoft.com?subject=IPD%20-%20Active%20Directory%20Certificate%20Services).