Windows Server 2003

Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure

David B. Cross and Carsten B. Kinder, Microsoft Corporation

Acknowledgements

Darren Canavor, Software Test Engineer, Microsoft Corporation

Jan de Clercq, Security Consultant, HP Consulting

Mike Lonergan, Consultant, Microsoft Consulting Services

Jason Hoffbuhr, Software Test Engineer, Microsoft Corporation

Ayman AlRashed, Consultant, Microsoft Consulting Services

Caesar Cunningham, Consultant, Microsoft Consulting Services

Brian Komar, Microsoft Corporation

About This Document

This document is a quick start guide that you can use to set up a Microsoft® Windows® Server 2003 public key infrastructure (PKI). It provides all the information that you need to deploy a viable PKI that is based on Windows Server 2003 technology.

The document outlines a proven PKI architecture that is applicable for the majority of organizations. It includes tips and decision best practices that have been obtained from customer experiences.

To ensure that configuration steps have been implemented correctly, this document also includes useful verification steps. Where possible, information regarding the configuration and installation of a server running a member of the Windows 2000 Server family is provided for comparison.

Document Structure

This document is based on "Designing a Public Key Infrastructure," in the *Microsoft Windows Server 2003 Deployment Kit* that is listed in the "Related Information" section in this document. Some issues are addressed only in the *Microsoft Windows Server 2003 Deployment Kit* chapter, while other issues are described only in this document. The similar structure provides easier navigation through the planning and deployment phase if you work with all of these documents.

> **Important** This document refers to features included with Windows Server 2003, Standard Edition, and Windows Server 2003, Enterprise Edition. These features are not included on computers running Windows Server 2003, Web Edition.

Scope

This document provides implementation guidelines for administrators who are deploying a Windows Server 2003 PKI in their organization.

This white paper is not an introduction to public key technologies, certification authorities, or certificates. It assumes that the reader has a good understanding of PKI and Active Directory concepts.

Because this white paper is focused on technology, it does not outline organizational guidelines and rules that are mandatory for a successful PKI implementation. You should apply organizational requirements and best practices in conjunction with the recommendations in this white paper to ensure a successful deployment.

A number of detailed best practices that are combined with real-world field experience from Microsoft and Hewlett Packard Consulting Services have been incorporated into this white paper.

Related Information

This documentation extends the "Designing a Public Key Infrastructure" chapter in the *Microsoft Windows Server 2003 Deployment Kit*, which contains overall PKI planning and design, and the Windows Server 2003 Help topics, which contains checklists and configuration information. The chapter in the *Microsoft Windows Server 2003 Deployment Guide* focuses on broad deployment considerations.

Overview of the PKI Design Process

Designing a PKI involves the following steps which may or may not be performed in this order:

- Outline the business scenario
- Define the application certificate requirements
- Create certificate policies and practices statements

- Design the certification authority (CA) infrastructure
- Create a certificate renewal strategy
- Develop a CA management plan

Integration Into Existing Environments

When you combine client computers running Microsoft Windows 2000 Professional or Microsoft Windows XP Professional and computers running a member of the Windows Server 2003 family, you have a range of PKI enhancements that let you securely extend your network to employees, partners, customers, and services. It enhances the management and performance features of the Windows 2000 security infrastructure. Windows XP Professional and the Windows Server 2003 family offer many PKI-specific business benefits to organizations that require secure business processes and IT infrastructures.

The base set of features is provided in the Windows Server 2003 family, and enhanced certification authority functionality is provided in Windows Server 2003 Server, Enterprise Edition, and Windows Server 2003 Server, Datacenter Edition. The PKI that is part of the Windows Server 2003 release is an improved version of the Windows 2000 PKI functionality. Nevertheless, you can combine a Windows Server 2003-driven PKI with an existing Windows 2000 Active Directory environment and certification authority (CA) infrastructure.

Client computers running either the Windows 2000 or Windows XP operating systems will benefit the most from a Windows Server 2003 PKI deployment, along with hardware devices that support the Windows environment. For more information on the capabilities of each client, see the Windows Server 2003 Help.

Determining Secure Application Requirements

The Windows Server 2003 Standard and Enterprise Editions include a full-featured PKI that delivers the business benefits of current public key cryptography. Users, computers, and services benefit from encryption and signing capabilities.

The Windows Server 2003 PKI supports a broad range of applications, including:

- Secure logon with smart cards
- Confidential and secure e-mail
- Secure code
- Trusted, on-demand access to network resources for remote users and trusted, permanent network connectivity for remote offices with network security, including remote access, virtual private networks (VPN) and wireless authentication
- File protection in the event of stolen or lost portable computers and other storage devices
- Access control and single-identity authorization across a range of Web and application servers
- Digital signatures that enable tamper-proof, legally-binding transactions
- Scalable technology to support millions of users and high-volume digital signature transactions

For more information about how the Windows PKI supports these applications, see the following articles on the Microsoft Web site:

- How PKI Works on the Microsoft TechNet Web site
- Microsoft Windows 2000 Public Key Infrastructure Introduction on the Microsoft TechNet Web site
- Applications Overview on the Microsoft TechNet Web site

The Windows Server 2003 PKI solution has several advantages over commercial third-party PKIs that are not part of the operating system and must be purchased separately. Users and access control are managed centrally through Active Directory, which simplifies the overall PKI management burden. Further, a Windows Server 2003 PKI does not require either per-certificate or per-user license fees that would raise the total cost of ownership (TCO) of the system. The PKI functionality in the Windows Server 2003 family integrates very well with many other features of the operating system.

Windows Server 2003 PKI and Dependencies

From a technical perspective, a Windows Server 2003 PKI has some requirements before you can deploy it. This section describes fundamental process information and installation details for a successful Windows Server 2003 PKI implementation.

New Features of a Windows Server 2003 CA

Windows XP and Windows Server 2003 environments can benefit the most from all of the features of the Windows Server 2003 certification authority (CA), but mixed configurations with earlier versions of Windows are also supported, with a little less functionality.

The following table lists the features that are described later in this section. These features are available through the CA if the CA is installed on a specific version of the operating system.

Table 1 PKI feature support with a CA that is installed on different versions of the operating system

	Windows Server 2003, Enterprise Edition or Datacenter Edition	**Windows Server 2003, Standard Edition**	**Windows 2000 Server**
V2 templates	Enterprise CA only	Not supported	Not supported
Key archival and recovery	Supported	Not supported	Not supported
Auto-enrollment	Both user and computer certificates supported	Computer certificates supported	Computer certificates supported
Delta certificate revocation lists (CRLs)	Supported	Supported	Not supported
Qualified subordination	Supported	Supported	Not supported
Role separation	Supported	Not supported	Not supported

Note Windows Server 2003, Web Edition does not include certification authority functionality, but may be used as a PKI client.

The following table lists the features that can be used at the client with a given CA infrastructure:

Table 2 PKI features that are available to clients

	Windows XP Professional client		**Windows 2000 Professional client**	
	Windows 2000 CA	**Windows Server 2003 CA**	**Windows 2000 CA**	**Windows Server 2003 CA**
V2 templates	Not supported	Supported	Not supported	By Web enrollment support only
Key archival and recovery	Not supported	Supported	Not supported	By Web-enrollment support only
Auto-enrollment	User: Not supported Computer: Supported	User: Supported Computer: Supported	User: Not supported Computer: Supported	User: Not supported Computer: Supported
Delta CRL	Not supported	Supported	Not supported	Not supported
Qualified subordination	Not supported	Supported	Not supported	Not supported

If your browser does not support inline frames, click here to view on a separate page.

For additional information, see the following articles:

- PKI Enhancements in Windows XP Professional and Windows .NET Server on the Microsoft Web site
- What's New in Security for Windows XP Professional and Windows XP Home Edition on the Microsoft Web site
- Data Protection and Recovery in Windows XP on the Microsoft Web site

Version 2 Templates

Templates are the building plan for certificates. A template turns a certificate request into a certificate signed with the CA's private key. For example, a template defines the validity time of a certificate and the certificate's subject name.

The most significant difference between the version 1 (V1) and version 2 (V2) templates is that V1 templates are predefined and unchangeable. With V2 templates, a CA administrator is able to configure a wide range of settings that apply during certificate enrollment, such as minimum key length, subject name definition, enrollment requirements like enrollment agent signature, and so on.

V2 templates are available only with an enterprise CA that is running Windows Server 2003, Enterprise Edition or Datacenter Edition. An enterprise CA that is running Windows Server 2003, Standard Edition does not support V2 templates.

Generally, templates are stored in the Active Directory configuration naming context and are usable with any CA in an Active Directory forest if they are assigned to the CA. A single set of templates are available for use by all CAs in the forest. However, V2 templates can only be utilized with Windows Server 2003, Enterprise Edition or Datacenter Edition CAs.

To use V2 templates, the Active Directory schema must be extended to the Windows Server 2003 schema in the forest. If the Active Directory environment consists of Windows Server 2003 domain controllers only, no action is required to benefit from a Windows Server 2003 PKI. If all domain controllers of a forest that hosts the Windows Server 2003 CAs are running Windows 2000 Server, you must also install Microsoft Windows 2000 Service Pack 3 (SP3) or later on all domain controllers, in addition to the new Windows Server 2003 schema definitions. For more information on how to upgrade the schema, see "Prepare the Active Directory environment" in this document.

- For more detailed information about certificate templates, their usage, and their definition capabilities, see "Certificates" in the Windows Server 2003 Family Help.
- For more information about Web enrollment support, see "The Step-by-Step Guide to Certificate Services Web Pages" on the Microsoft TechNet Web site.
- For more information about certificate enrollment, see "Certificate Enrollment" in the "MS Windows 2000 Public Key Infrastructure Introduction" white paper on the Microsoft TechNet Web site.
- For more information about extending the schema for V2 templates, see the Windows Server 2003 Help topics regarding certificate templates.

Certificate Enrollment

You can enroll V2 templates with any computer running Windows XP or later through the default enrollment methods, including the Certificates Microsoft Management Console (MMC), the built-in auto-enrollment mechanism, Web enrollment support, or command-line tools.

A computer running Windows 2000 cannot use the Certificates MMC to enroll a V2 template. However, any client that is running Microsoft Internet Explorer 5.01 or later can use a V2 template to enroll certificates through the Web enrollment methods and a downloaded ActiveX control. To download the ActiveX control on a client computer, it is necessary to log on as an Administrator or Power User on the local computer. In addition, clients running Windows 2000 can enroll V2 templates through a Terminal Server connection running on an appropriate member of the Windows Server 2003 family.

> **Note** An enrollment agent that enrolls certificates that are based on V2 templates requires either a Windows XP or Windows Server 2003 enrollment station. There is no support to enroll V2 templates with an enrollment agent on a Windows 2000 enrollment station. Nevertheless, certificates that are based on V2 templates that have been enrolled through an enrollment agent on either a Windows XP or Windows Server 2003 enrollment station can be used on a Windows 2000 client computer.

If certificates have been enrolled with a Windows 2000 PKI where only V1 templates were available, there is no immediate need to re-enroll or renew these certificates with V2 templates.

The following table lists different enrollment methods that are supported on computers that are running Windows 2000, Windows XP, or the Windows Server 2003 family. You can use scripted enrollment with support of CAPICOM and Xenroll. (CAPICOM and Xenroll documentation, including samples, can be found on the Microsoft Developer Network (MSDN) Web site.)

Table 3 Certificate Enrollment

	Certificates MMC	Web-enrollment	Scripted enrollment
Self enrollment on a Windows 2000 workstation	V1 template: Yes V2 template: No	V1 template: Yes V2 template: Yes	V1 template: Yes V2 template: Yes

Self enrollment through a Windows Server 2003 Terminal Server session	V1 template: Yes V2 template: Yes	V1 template: Yes V2 template: Yes	V1 template: Yes V2 template: Yes
Enrollment agent on a Windows 2000 workstation	V1 template: No V2 template: No	V1 template: Yes V2 template: No	V1 template: No V2 template: No
Enrollment agent through a Windows Server 2003 Terminal Server session	V1 template: No V2 template: No	V1 template: Yes V2 template: Yes	V1 template: No V2 template: No

Note Because a PKI is a forest resource, the Active Directory site structure is not taken into account when any kind of certificate is requested and issued. An Active Directory–integrated certificate requester enumerates all registered enrollment services in Active Directory and sends its request to a CA that can enroll the certificate type that the user wants. The client does not necessarily choose the closest CA, from a network perspective. Because of this, you should verify that the CA deployment ensures that any client has reliable network connectivity with a CA.

User Certificate Autoenrollment

Autoenrollment provides a quick and simple way to issue user certificates and to benefit from applications that can use PKI. User autoenrollment also minimizes PKI deployment costs.

Certificate autoenrollment also works in a Terminal Server session if you use a Windows Remote Display Protocol (RDP) 5.1 client.

When you use a computer that is running Windows XP, you can automatically enroll users and computers for certificates, including smart card-based certificates. In contrast, the Windows 2000 Server family only supports certificate autoenrollment for computer certificates. User certificate auto-enrollment builds on the standard Windows security model for domain authentication and authorization. This model may not be suitable for all certificate issuance or scenarios.

Using the new autoenrollment feature, organizations can manage the certificate lifecycle through V2 templates for users. This includes:

- Certificate renewal
- Superseding of certificates
- Multiple signature requirements

Depending on the configuration of the template that is used for autoenrollment, the user can be notified when a certificate enrollment or renewal is performed.

Certificate autoenrollment is based on the combination of Group Policy settings and V2 certificate templates. This combination allows certificate enrollment and renewal in the background for computers and users at any time when you apply Group Policy.

To perform autoenrollment, the certificate requester must be registered and authenticated as either a user or computer in Active Directory.

For more information, see "Certificate Autoenrollment in Windows Server 2003" on the Microsoft TechNet Web site.

Certificate Renewal

When a certificate comes to the end of its lifetime, it must be renewed or replaced to ensure that the certificate owner is able to continue with the certificate's purpose.

In certificate renewal, the renewal requester already owns a certificate. The renewal takes the information of the existing certificate into account when the renewal request is submitted. A certificate can either be renewed with a new key or the existing key can be used for the renewed certificate.

If a certificate was enrolled with a V2 template, it cannot be renewed if it was based on a V1 template. However, a certificate that was enrolled with a V1 template can be renewed with a certificate that was made from a V2 template.

Table 4 Certificate Renewal

	Certificates MMC	**Web-enrollment**	**Scripted enrollment**
Self renewal on	V1 template: Yes	V1 template: No	V1 template: Yes

Windows 2000 workstation	V2 template: No	V2 template: No	V2 template: Yes
Self renewal on Windows 2000 workstation with Windows Server 2003 Terminal Server session	V1 template: Yes V2 template: Yes	V1 template: No V2 template: No	V1 template: Yes V2 template: Yes
Renewal with enrollment agent on Windows 2000 workstation	V1 template: No V2 template: No	V1 template: No V2 template: No	V1 template: No V2 template: No
Renewal with enrollment agent on Windows 2000 workstation with Windows Server 2003 Terminal Server session	V1 template: No V2 template: No	V1 template: No V2 template: No	V1 template: No V2 template: No

Key Archival and Recovery

Key archival and recovery is only available for encryption certificates by V2 templates, because the archival option must be individually set for each template. Key archival is most often used for encryption keys that are used to protect persisted data.

Private keys that are associated with certificates that are used only for digital signature are not archived and are blocked by the certification authority. The archival and recovery function that is available with the Microsoft Exchange 2000 Key Management Server (KMS) has been replaced by the enterprise CA running Windows Server 2003, Enterprise Edition.

The enterprise certification authority on a computer that is running Windows Server 2003, Enterprise Edition, supports migration of the archive database from the Exchange 2000 KMS to ensure a smooth transition of technologies.

Encrypting File System (EFS) will continue to support decentralized data recovery methods as well as key archival on clients that are running Windows XP.

Delta CRLs

Delta certificate revocation lists (CRLs) decrease the network traffic that is caused when a new certificate revocation list needs to be downloaded. Without delta CRLs, a client must receive the base CRL that contains all certificates that are revoked by a CA. To decrease the CRL's size and make more frequent updates valuable, delta CRLs only retain the certificates that have been revoked since the last publication of the base CRL.

Some limitations apply to delta CRLs:

- Delta CRLs are issued by Windows Server 2003 stand-alone and enterprise CA's.
- Only clients that are running Windows XP Professional and later are able to check the validity of certificates against delta CRLs.

For more information on this topic, see "Troubleshooting Certificate Status and Revocation" on the Microsoft TechNet Web site.

Qualified Subordination

Qualified subordination allows cross-certification of CA certificates with name constraints and provides for more precise control of certificate trusts. With qualified subordination, an administrator can also include or exclude certificate purposes. For example, qualified subordination might reject Internet Protocol security (IPSec) usage with a third-party certificate, but allows secure e-mail with the same certificate, even if the certificate's key usage would allow IPSec and secure e-mail.

Qualified subordination requires a Windows XP or Windows Server 2003 operating system as the certificate requester and a Windows Server 2003, Enterprise Edition CA.

Simple Certificate Enrollment Protocol

You can implement secure networking with the Simple Certificate Enrollment Protocol (SCEP), which is provided as an add-on component in the Windows Server 2003 Resource Kit. The Microsoft SCEP (MSCEP)

component is an Internet Server Application Programming Interface (ISAPI) filter that uses Microsoft Internet Information Services (IIS) and is installed directly on a CA to support the SCEP enrollment protocol with network devices.

For more information, see article 249125, "Using Certificates for Windows 2000 and Cisco IOS Interoperation," in the Microsoft Knowledge Base.

Role Separation

There are a number of tasks in the PKI process that you should understand:

- **Certificate enrollment**. Sends a certificate request to the CA, and then the CA issues the certificate and then deploys a certificate to the certificate holder.
- **Certificate renewal**. Sends a request to renew an existing certificate to the CA, the CA issues the certificate, and then the CA deploys a certificate to the certificate holder.
- **Certificate revocation**. Revokes certificates and publishes the certificate revocation list (CRL).
- **Recovery**. Provides the certificate holder with both a certificate and a key that are stored in the CA database.

There are also a number of roles that are related to a Windows Server 2003 CA, although you may not need all of these roles:

- The **CA manager** maintains the CA and its configuration.
- The **CA administrator** delegates certificate-management permissions to Certificate Managers.
- The **certificate manager** issues and revokes certificates.
- The **enrollment agent** requests and deploys certificates.
- The **certificate holder** requests self-maintained certificates and is able to use the certificate.
- The **recovery agent** recovers certificates for specific applications, such as EFS.

The following table shows which role can perform a particular task and what permissions are required to perform that function. The top row lists various roles, and the left column lists the tasks. The table text describes the permission that is required to perform each task.

Table 5 Certificate Roles and Tasks

	Certificate Holder	Enrollment Agent	Recovery Agent	Certificate Manager	CA Manager
Maintain	Not applicable	Not applicable	Not applicable	Not applicable	Requires CA Manager permissions on the CA object
Request	Requires certificate holders membership on the certificates template ACL	Requires certificate holders membership on the certificates template ACL	Not applicable	Not applicable	Not applicable
Renew	Requires certificate holders membership on the certificates template ACL	Requires certificate holders membership on the certificates template ACL	Not applicable	Not applicable	Not applicable
Issue	Not applicable	Not applicable	Not applicable	Certificate Manager permission on a template	Not applicable
Revoke	Not applicable	Not applicable	Not applicable	Certificate manager permission	Not applicable
Recover	Not applicable	Not applicable	Key recovery agent certificate	Not applicable	Not applicable

CA Permissions

For a Windows Server 2003 stand-alone CA that is installed on a server that is not a member of an Active Directory domain, local administrator permissions are mandatory to manage the CA functions.

On a server that is a domain member, the user who installs an enterprise CA must be a member of the Active Directory Root Domain Admins and Enterprise Admins security group. You should ensure that the installation account is a member of both security groups. This set of permissions is required for any enterprise CA installation, and it assumes that the Enterprise Admins group or Domain Admins group also is a member of the local server Administrators group. To install a stand-alone CA, only local administrator privileges are required.

During setup, containers and objects that contain enrollment and CA information are created as part of the configuration container of Active Directory. For a list of object default permissions that are used by a CA, see article 239706, "Default Permission Settings for Enterprise Certificate Authority," in the Microsoft Knowledge Base.

It is recommended that you use only the Certification Authority MMC to change security permissions for the CA. If you use other mechanisms, such as the Active Directory Sites and Services MMC, you may cause an unsupported environment due to a configuration mismatch between Active Directory and the local CA registry. The Certificate Templates MMC ensures consistency in the ACLs. If ACLs are changed manually, specific permissions may be missing and the CA will not function as expected.

Command-line Administration Tools

Command-line administration tools are part of the Windows Server 2003 family and may be installed on computers running Windows XP and later through the Windows Server 2003 Administration Tools Pack, which is available on the Windows Server 2003 installation media. Command-line tools that are required for CA administration on Windows 2000 operating systems are only installed with Windows 2000 Certificate Services. For more information about **Certutil.exe** and **Certreq.exe**, including a description and the necessary syntax, see the Windows Server 2003 Help.

CA Fault Tolerance

Generally, you should use certification authority fault tolerance because:

For online CAs, it provides certificate issuance services.

For both online and offline CAs, it provides certificate revocation information.

Neither Windows 2000 nor Windows Server 2003 technology supports native clustering of the CA database or certificate services. Only one CA instance can be installed at a time on a server running a Windows Server 2003 operating system.

An enterprise CA is designed to provide natural fault tolerance in an Active Directory environment. If one enterprise CA does not work or is not available, client services will automatically attempt enrollment with the next available enterprise CA in the forest. No errors are generated and no user interaction is required. For more information, see "Online Enterprise Issuing CAs" later in this document.

If a CA is not available because of a hardware failure, for example, it might still be necessary to publish the CRL on a regular basis. The CRL publication interval depends on the CA configuration. If the CA does not publish the CRL in time, clients cannot verify certificates against the latest version of the CRL.

To publish a CRL on behalf of a CA, you must own the CA private key. If the CA private key has been exported to a file, it is technically possible to resign a CRL on behalf of the CA and extend the lifetime of the CRL.

> **Note** Exporting the CA private key could raise a security risk because the owner of the CA's private key is able to act on behalf of the CA. The CA private key must be maintained very carefully and must be stored in a secure vault that is protected through secure and audited processes.

Deployment Planning

Before you can deploy a PKI, you should go through a well-defined planning phase. If you do not do this, the PKI can become valueless after only a short time in operation. To avoid this issue, make sure that the deployment planning covers the following areas.

Table 6 PKI Planning Considerations

Planning area	Possible considerations
Business requirements	Defining application requirement Defining solutions goals Choosing appropriate technology
CA requirements	Insource the CA infrastructure

	Outsource the CA infrastructure Interoperability with application requirements PKI trust model
Enrollment policy	Certificate practice statements Users and computers Use of certificate templates Service level requirements
Revocation policy	CRLs, delta CRLs, Online Certificate Status Protocol (OCSP) Replication latency Disaster recovery procedures

Designing the CA Infrastructure

For more information about how to decide what services are provided by the CA types, see the articles on the following Microsoft Web sites:

- "MS Windows 2000 Public Key Infrastructure Introduction" on the Microsoft TechNet Web site
- "An Introduction to the Windows 2000 Public-Key Infrastructure" on the Microsoft Web site
- "Cryptography and Microsoft Public Key Infrastructure" on the Microsoft TechNet Web site
- "Planning Your Public Key Infrastructure" on the Microsoft TechNet Web site

Considerations

There are some important parameters that help when a organization starts its PKI planning. From a technical viewpoint, there are a number of key factors that can give you rough estimates:

The number of CAs that you need can be estimated by:

- The size and the geographical spread of the deployment
- The required trust relationship between certificate holders and the CA
- Requirements for different certificate practice statements (CPS)
- Technical requirements based on application demands
- Partner relationships and trust model requirements
- Security requirements, availability, and service levels indicate the depth of the hierarchy and the CA locations.

Defining CA Types and Roles

To plan your CA infrastructure, you need to understand the different types of CAs that are available and the roles that the CAs can take.

The following section supplies the most important planning information.

Choosing Enterprise or Stand-alone CAs

Certificate Services offers two types of CAs that have different feature sets: enterprise CAs and stand-alone CAs. A Windows Server 2003 PKI may consist of both types of CAs, which is often recommended for the enterprise environment. A comparison of strengths of the stand-alone CA and the enterprise CA may help you decide what CA type is required for which role.

A stand-alone CA should be used if:

- It is an offline root or offline intermediate CA.
- Support of templates that you can customize is not required.
- A strong security and approval model is required.
- Fewer certificates are enrolled and the manual work that you must do to issue certificates is acceptable.
- Clients are heterogeneous and cannot benefit from Active Directory.
- It is combined with a third party Registration Authority solution in a multi-forest or heterogeneous environment

- It issues certificates to routers through the SCEP protocol

An enterprise CA should be used if:

- A large number of certificates should be enrolled and approved automatically.
- Availability and redundancy is mandatory.
- Clients need the benefits of Active Directory integration.
- Features such as autoenrollment or modifiable V2 templates are required.
- Key archival and recovery is required to escrow encryption keys

The following table is an overview about the preferred roles for both CA types. Depending on the CA topology, these roles can be taken by a smaller or larger number of CAs.

Table 7 CA Types and CA Roles

CA type	3 tier	2 tier	1 tier
Offline root CA	Stand-alone CA	Stand-alone CA	Enterprise CA
Offline intermediate CA	Stand-alone CA		
Issuing CA	Enterprise CA	Enterprise CA	

Table 8 Comparison of Stand-alone and Enterprise CAs

Windows Server 2003 Stand-alone CA	Windows Server 2003 Enterprise CA
CA configuration can be published into Active Directory.	CA configuration is always published into Active Directory.
CRL and CA certificate must be manually published into Active Directory.	CRL, Delta CRL, CA certificate, and cross certificates are automatically published to the forest where the CA configuration was registered. Certificates are automatically published into a directory service if this is specified on a per template level. Certificate publishing may be defined as an attribute on the template in Active Directory.
By default, certificate enrollment is available only by using Web enrollment support.	By default, certificate enrollment is possible by using Web enrollment or the Certificates MMC.
Certificate request processing is done by using Hypertext Transfer Protocol (HTTP) or Secure Hypertext Transfer Protocol (HTTPS).	Certificate request processing is done primarily by using RPC/Distributed Component Object Model (DCOM) or HTTP and HTTPS protocol.
Certificate is based on V1 templates with custom object identifier (also known as OID).	Also issues certificates that can be modified and duplicated, based on V2 templates .
User must manually type identification information when the certificate is requested.	User identification information is always automatically retrieved from Active Directory, regardless of whether it is requested through Web enrollment or the Certificates MMC.
Enrollment method (automatic or pending) is valid for all templates. You cannot apply a configuration to individual templates.	You can individually set the enrollment method on each template.
Certificates are manually approved.	Certificates are manually approved or they are approved through Active Directory authentication and access control.
Certificates are not published to a directory location, but to the client or the CA. without a custom-developed policy module.	Depending on the type of certificate, certificate is automatically enrolled into the requester’s certificate store and published to Active Directory, based on template definition.
Does not support certificate publishing and object management based on Active Directory.	Supports certificate publishing and object management based on Active Directory.
Can be installed on a domain controller, member	Can be installed on a domain controller or member

server, or stand-alone server (workgroup member).	server. (The CA is registered as a forest resource.) It must not be installed on a stand-alone server (workgroup member).

Authentication and Authorization

Stand-alone CAs use local authentication for certificate requests, mainly through the Web enrollment interface. Stand-alone CAs provide an ideal service provider or commercial PKI provider platform for issuing certificates to users outside of an Active Directory environment where the user identity is separately verified and examined before the request is submitted to the CA.

A CA running Windows Server 2003, Enterprise Edition, uses DCOM and Kerberos impersonation for authenticating requesters. It compares the client token against an access control list (ACL) set on the certificate template, as well as the DCOM enrollment interface on the CA itself, when a certificate is requested. A Windows 2000 Server CA uses remote procedure call (RPC) instead of DCOM to authenticate a requester. After the user is authenticated and authorized to gain access to the requested template, the CA can immediately process the request, as long as the user has the appropriate enrollment permissions on the template and if the CA's configuration is set to autoenroll.

Certificate Request Approval

When a certificate request reaches a CA that is running a member of the Windows Server 2003 family, both CA types (enterprise and stand-alone) can immediately issue the certificate or put it into a pending state. It is the responsibility of the CA administrator to configure the enrollment method globally for a CA or on a per-template basis. On a Windows 2000 Server CA, the enrollment method setting is valid only on a CA level: all certificates that are issued take this configuration into account. For a Windows Server 2003, Enterprise Edition enterprise CA, the enrollment method can be set individually for a V2 template.

On a Windows 2000 Server enterprise CA, there is no choice for the enrollment method because it immediately approves and issues certificates. On a Windows 2000 Server stand-alone CA, the enrollment method is applied on the CA level and cannot be set on the template level This occurs because a Windows 2000 CA works only with V1 certificates, which cannot maintain enrollment permissions.

Default configurations of stand-alone CAs rely on administrative action both to verify the requester's identity (known as *authentication*) and to issue the certificate (known as *authorization*). Here, the Web enrollment support acts as the registration authority (RA) and the CA acts as the enrollment station. Because of this, it is not recommended that you have a standalone CA automatically issue certificates without administrative approval, because a requester's identity cannot be verified. For additional information about certificate enrollment, see "Allowing for autoenrollment" in Help and Support Center.

Offline and Online CAs

Traditionally, the decision of whether to use either an online or offline CAs involves a compromise between availability and usability versus security. The more sensitive that the key material is and the higher the security requirements are, the less accessible the CA should be to users.

> **Important** For security reasons, a CA should always run on a separate computer. Do not install an online CA on a domain controller, even if it is technically possible.

To maintain a CA offline, different approaches may be applied through physical or technical protection techniques as described below:

Physical Protection

- Remove the hard disk drive and lock it in a secure location.
- Shut down and power off the system.
- Disconnect the network cable, but keep the system running.
- Protect the system from the network by using either a firewall or a router.

Technical Protection

- Keep the system online, but stop the CA service.
- Use a hardware security module (HSM) with an HSM-operator hardware token to limit access to the CA private key. For more information, see "Hardware CSPs," later in this document.

Maintaining a CA either online or offline is a standard functional definition of the CA's operation mode. You can turn an offline stand-alone CA into an online stand-alone CA if you connect it to the network. Any stand-alone CA that runs on a server in a workgroup and is connected to the network can become an offline CA by using one of the approaches that was mentioned earlier.

The stand-alone root CA is usually placed offline because it is the single point of trust for an entire organization

or for several organizations. The lifetime of trust depends on the CA's certificate lifetime, but should be planned for the long term. If a CA must be trusted for long periods of time, you should take that CA offline to provide additional security measures. Also, intermediate CAs are typically configured as offline CAs. An intermediate CA is subordinate to a root CA, but also serves as a parent CA to one or more CAs. Those CAs may be issuing CAs or intermediate CAs. In a CA with at least three tiers, an intermediate CA is a mid-tier CA.

Every online CA implies availability and network connectivity. Online CAs are typically issuing CAs, because issuing CAs respond to requests from users, computers, services, and network devices, such as routers. Every enterprise CA must be an online CA, because it requires connectivity to Active Directory at all times to obtain configuration information, validate requests, and publish certificates. An online CA provides more surface area for security attacks.

Note As a best practice, an offline CA server should be placed in a secure vault until a subordinate CA certificate needs to be issued or a new CRL needs to be published.

Hardware CSPs

You might consider using one or more HSMs in your PKI topology. An HSM is a dedicated hardware device that is managed separately from the operating system. These modules work with any Windows Server 2003 CA to provide a secure hardware store for CA keys. From an operating system view through the CryptoAPI interfaces, the HSM is seen as a cryptographic service provider (CSP) device.

The HSM provides highly secure operational management that is protected by multilayered hardware and software tokens, as well as a number of other key features, including:

- Hardware-based, cryptographic operations, such as random number generation, key generation, and digital signatures, as well as key archival and recovery.
- Hardware protection of valuable private keys that are used to secure asymmetric cryptographic operations.
- Secure management of private keys.
- Acceleration of cryptographic operations, which relieves the host server of having to perform processor-intensive, cryptographic calculations.
- Load balancing and failover in hardware modules by using multiple HSMs that are linked together through a daisy chain.

Although HSMs increase security by raising the level of key protection, HSMs increase the complexity and cost of the PKI.

Several vendors offer HSMs that work well on computers that are running either Windows 2000 Server or members of the Windows Server 2003 family. For more information about how to install HSMs that are proven to work with Windows-based CAs, see the section "Installing an HSM on an offline root CA" later in this document.

Selecting A Trust Model

Trust is a logical relationship established between domains to allow pass-through authentication, in which a trusting domain honors the logon authentications of a trusted domain. User accounts and global groups that are defined in a trusted domain can be given rights and permissions in a trusting domain, even though the user accounts or groups don't exist in the trusting domain's directory. Because a CA is a certificate holder of a CA certificate and an end entity might be a certificate holder of a user certificate, the trust relationship between the issuing CA and the holder is always the same. In a rooted x.509 PKI hierarchy, the trust relationship is inherited from top to bottom.

You can also control trust relationships through *certificate trust lists* and through qualified subordination. (For more information, see the slide presentation "Certificate Trusts Lists" at the National Institute of Standards and Technology (NIST) Web site. The selection of an appropriate trust model can determine success for a PKI. An organization must think about the number of tiers that the CA topology requires. The hierarchy can be extended from top to bottom and the number of CAs that are used for one level can grow. Note that deeper structures add complexity to the trust management of the PKI.

Note Web addresses can change, so you might be unable to connect to the Web site or sites mentioned here.

For more information, see the article "Trusted Root Certificates That Are Required By Windows 2000" on the Microsoft Knowledge Base.

Specifying CA Roles

An ideal PKI hierarchy design divides the responsibility of the CAs. A topology that is designed with requirements that have been carefully considered provides the most flexible and scalable enterprise configuration. In general, CAs are organized in hierarchies. Single tier hierarchies might not provide adequate security compartmentalization, extensibility and flexibility. Hierarchies with more than three tiers might not

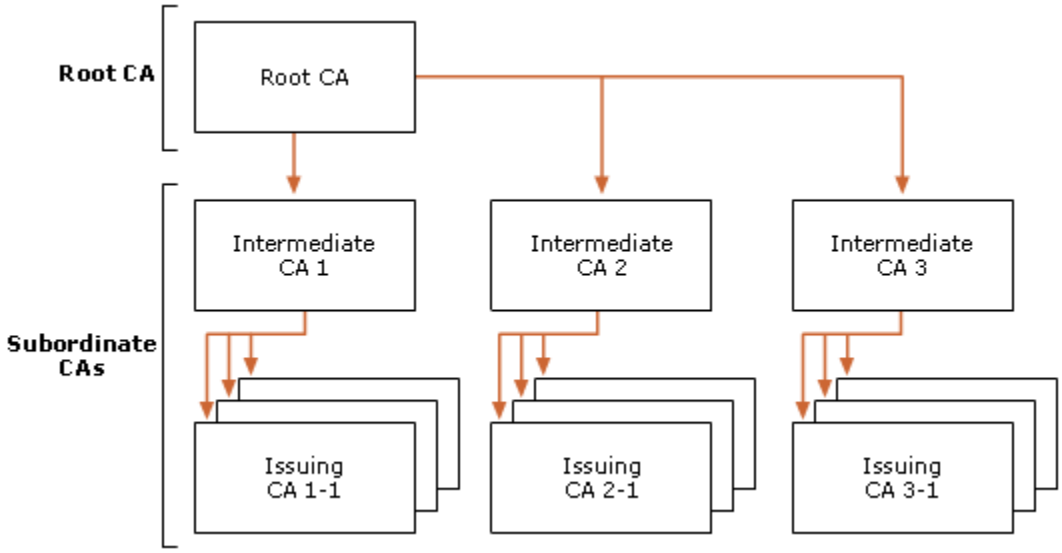
provide additional value regarding security, extensibility and flexibility.

The most important consideration is protecting the highest instance of trust as much as possible. Single-tier hierarchies are based on the need to compartmentalize risk and reduce the "attack surface" that is available to users who have malicious intent. A larger hierarchy is much more difficult to administer, with little security benefit.

Depending on the organization's necessities, a PKI should consist of two or three logical levels that link several CAs in a hierarchy. Administrators who understand the design requirements for a three-level topology may also be able to build a two-level topology.

A three-tier CA hierarchy consists of the following components:

- A root CA that is configured as a stand-alone CA without a network connection
- One or more intermediate CAs that are configured as stand-alone CAs without a network connection
- One or more issuing CAs that are configured as enterprise CAs that are connected to the network



If your browser does not support inline frames, click here to view on a separate page.

Figure 1 Three-tier CA Hierarchy

To set up a two-tier topology, apply all of the steps that are described in "Example scenario for Contoso Company," later in this document.

If the organization can fulfill its security requirements with a two-tier hierarchy, a three-tier architecture is not required. When you do not have a middle tier, CA management applies to two levels instead of three levels and might lower maintenance cost.

To implement a two-tier topology, use the steps that are outlined in both the "Stand-alone offline root CA" and "Online Enterprise Issuing CAs (CorporateEnt1CA)" sections of this paper.

From a technical perspective, a single level PKI hierarchy can also provide basic PKI services. Leaving out the root and the intermediate tier results in an all-in-one CA. Because the single CA must issue certificates, it cannot be taken offline. Security and flexibility is very limited with this type of implementation. To implement a single-tier topology, apply the steps that are outlined in "Online Enterprise Issuing CAs (CorporateEnt1CA)."

The decision of whether or not to use a separate root CA to issue all certificates in an organization should be a need for security versus a need for cost mitigation and simple administration.

To summarize, a two-tier to four-tier CA topology is the most common deployment. Any organization should be able to deploy a similar PKI architecture to meet any organizational, business, and technical requirement, as well as a respectable level of security.

For reliability and redundancy, improve the availability of the PKI and deploy multiple enterprise CAs instead of extending the depth of the hierarchy.

Root CA

A root CA is a self-signed CA. Technically, the root CA runs the same code as an intermediate or issuing CA. The difference between these types of CAs is in the role that the CA takes. The following table displays a list of the characteristics that a root CA should have, depending on the CA topology.

Table 9 Root CA Characteristics

Characteristic	More than 2 tiers	2 tiers	1 tier
High level of physical security	Yes	Yes	No
Permanently offline	Yes	Yes	No
Highly restricted area (vault)	Yes	Yes	Yes
Match the level of risk	Yes	Yes	Yes
High level of cryptographic security	Yes	Yes	Yes
Largest key size	Yes	Yes	Yes
Software CSP (FIPS 140-1 level 1)	No	No	Yes
Smart cards or PCMCIA tokens with PINs (FIPS 140-1 level 2)	No	Yes	Yes, recommended
Hardware security modules with operator hardware token (FIPS 140-1 level 3 or 4)	Yes	Yes, recommended	Yes, recommended

Even if an offline root CA might run only when the CA certificate must be renewed or the CRL has to be published, the CA must be installed on reliable hardware. If you are thinking about using a notebook computer to take the role of the root CA, note that it does not meet the requirements for reliability at the time that this document is being published.

In most customer environments, maintaining a root CA requires extraordinary security measures. The level of security requires that the root CA is offline at all times and, preferably, protected in a secure physical environment. In theory, a desktop system with a removable hard drive can be used to protect a root CA.

Intermediate CAs

Intermediate CAs are subordinate to the root CA. By definition, if you implement an intermediate CA, the topology consists of a minimum of three tiers . The intermediate layer of a PKI hierarchy often provides useful policy, administrative or operational differentiation. Intermediate CAs are also known as policy CAs because they are often used to manage or dictate different security and operational policies between different geographical regions, business units, or the intranet or extranet for a corporation.

To implement policies without an intermediate CA, you can also assign policies to issuing CAs on a logical basis.

An intermediate CA's security requirements are the same as for the root CA because an intermediate CA provides CA certificates to online issuing CAs. The intermediate CA should be a offline, stand-alone CA.

> **Tip** It is highly recommended that you only issue certificates from an intermediate CA after the administrator manually approves the request. This is is the default configuration for a Windows Server 2003 stand-alone CA.

Issuing CAs

Depending on the architecture, an issuing CA is a subordinate of an intermediate CA or a subordinate of the root CA. Enterprise CAs are ideal for issuing large numbers of certificates, because they can automatically validate the user and certificate profile information. The purpose of an issuing CA is to enroll certificates to end-entities and not to subordinate CAs.

> **Note** You can limit the number of subordinate CA levels in a certificate hierarchy by defining a maximum path length in the basic constraints extension of a CA certificate. A path length of zero will ensure that an issuing CA may only issue certificates to end-enties. You can define the basic constraints extension and path length by using a CApolicy.inf configuration file.

Understanding Root Trust

When a client uses a certificate, it is mandatory that the trust relationship between the certificate and the root CA can be verified. A certificate is trusted if the client that verifies the certificate trusts the root CA certificate that is in the client certificates certificate trust path as well. A client must have the related root CA certificate in its local certificate store to proof a trust-relationship with the root CA. For more information, see "Policies to establish trust of root certification authorities" on the Microsoft Web site.

If Active Directory is available, it is important to understand how clients like users or computers can benefit from Active Directory to establish a trust relationship with the root CA

You can achieve the trust that is obtained from a root certification authority by deploying the root CA certificate through one of the following six methods:

- Enterprise trust in Active Directory
- Group policy in Active Directory
- Certificate Trust Lists (CTLs) in Group Policy
- Manual trust on a local computer
- Manual trust by a user
- Windows Update

Depending on the permissions and the scope of the distribution mechanism, certificates are put into different locations and require different maintenance tools. For more information, see the following table.

Table 10 Certificate Trust Mechanisms

Distribution method	Scope	Uses Group Policy Object	Location	Maintained with
Enterprise trust	Entire forest	Yes	Services\Public Key Services\CertificationAuthorities	**Certutil.exe** or PKI Health Tool (Available in the Windows Server 2003 Resource Kit.)
Group policy trust	Domain	Yes	Domain Security Group Policy object	Group Policy MMC
NTAuth (for CAs trusted to issue authentication certificates)	Entire forest	Yes	Services\Public Key Services\NTAuth object	**Certutil.exe** or PKI Health Tool (Available in the Windows Server 2003 Resource Kit.)
Manual trust on the local computer	Local computer and all users that log on to system	No	Registry HKEY_LOCAL_MACHINE	Certificates MMC for the local computer
Manual trust by user	Current user	No	Registry HKEY_CURRENT_USER	Certificates MMC for the local computer
Windows Update	Local computer and all users that log on to system	No	Registry HKEY_LOCAL_MACHINE	Group Policy MMC or **Add or Remove Programs** in Control Panel

Enterprise Trust

You can use the built-in autoenrollment service to automatically download root CA certificates and certificate trust lists (CTLs) from the Active Directory enterprise trust store on both Windows 2000 and Windows XP clients.

For additional information, see the following articles on the Microsoft Web site:

- Certificate Autoenrollment in Windows Server 2003 on the Microsoft TechNet Web site
- Configure Public Key Group Policy on the Microsoft Web site

Group Policy Trust

Group Policy trust is defined and configured by using the Group Policy MMC and the Default Domain Security

Group Policy object. Group Policy trust is configured and enforced for the domain where the Group Policy object applies. Because of this, different users in different domains trust different root CAs. It is highly recommended to create a new domain policy and not edit the default domain policies.

Note Only root CA certificates must be trusted and registered on client computers. Do not add subordinate CA certificates to the Group Policy trust, because intermediate and issuing CAs certificates may not be explicitly trusted. CryptoAPI automatically builds certificate chains for subordinate and intermediate CA certificates with the Authority Information Access (AIA) extension.

NTAuth

The NTAuth store is deployed on all computers in the forest from the configuration partition of the forest in the following directory path:

CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration,DC=...

Important NTAuth CAs are trusted to both issue authentication (logon) certificates for any user in the forest and enable logon for smart cards, Internet Information Services (IIS) mapping, and Extensible Authentication Protocol-Transport Layer Security (EAP-TLS).Precise control of issuing CAs can be achieved through qualified subordination with constraints.

You can verify the certificates that are currently registered in NTAuth by typing the following at a command prompt where the domain component information is configured with the name of the Active Directory root domain:

certutil.exe -store ldap:///CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration,DC=contoso,DC=com

You can see a more visual display of certificates by typing the following at a command prompt:

certutil -viewstore "ldap:///CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration,DC=..."

You can also manually maintain the NTAuth store by typing one of the following commands at a command prompt:

certutil –addstore

certutil –delstore

certutil –dspublish *CertificateFile* **NTAuth**

For more information about the NTAuth store and smart card logon, see the following articles on the Microsoft Web sites:

- "Step-by-Step Guide to Mapping Certificates to User Accounts" on the Microsoft TechNet Web site
- "How to Import a Third-Party Certificate into the NTAuth Store" on the Microsoft Knowledge Base
- "Enabling Smart Card Logon with Third-Party CAs" on the Microsoft Knowledge Base
- "Requirements for Third-Party CA Domain Controller Certificates" on the Microsoft Knowledge Base

In a Windows Server 2003 Active Directory environment that contains only clients running Windows XP, the NTAuth store is not mandatory for smart card logon and certificate mapping, compared to a Windows Server 2003 mixed environment with Windows 2000 clients. Because Windows Server 2003 Active Directory supports publishing cross-certificates and because clients running Windows XP support name and policy constraints for x.509 certificates, administrators may waive the NTAuth policy in homogenous Windows Server 2003 and Windows XP environments. This option requires and assumes that CAs have defined name constraints instead of being listed in the NTAuth store of the directory. Therefore, domain controllers that process both smart card logon and certificate mapping requests will explicitly trust all CAs that chain to trusted root CAs, assuming that the certificate matches a valid user account in Active Directory.

Caution Disabling NTAuth policy verification enables domain controller trust of any CA that issues a valid smart card logon certificate and chains to a trusted root CA in the Active Directory environment. Any CAs, including the default third-party root CAs, should have name constraints defined before disabling the NTAuth policy. If this does not occur, unintended trust and logon access may occur. Use this option with extreme caution and only when root CAs have been properly constrained in the environment.

For more information on qualified subordination and name constraints, see "Planning and Implementing Cross-Certification and Qualified Subordination Using Windows Server 2003" on the Microsoft TechNet Web site.

Manual Trust on a Local Computer

Root CA certificates may also be manually trusted on a local computer by using the Certificates MMC snap-in for the local computer. The user must be a local administrator to add root CA certificates to the machine certificate store. All root CA certificates in the computer's machine certificate store are inherited by all users who log on to that computer. The users trusted root certificate store and the machine trusted root certificate

store form a union from a users perspective.

For more information on certificate stores, see Chapter 13, "Public Key Technology" on the Windows 2000 Resource Kit Web site.

Confirm that certificates are stored in the correct location. Any root CA certificate that is stored in the local computer's certificate store is visible to any user on that computer. If a root CA certificate is registered in the local computer store and if the CA certificate is also manually added by a user, the root CA certificate might appear twice in the Certificates MMC snap-in. If a root certificate is not available in the local computer's certificate store but is available in the user's store, building a certificate chain also may not work for some applications.

You can maintain the computer's certificate store also with the Internet Explorer Administration Kit (IEAK) or CAPICOM. For more information about CAPICOM, see the article "CAPICOM Reference" on the MSDN Web site.

Manual Trust by User

It is recommended that only administrators maintain certificate trust and that you store only CA certificates in the local computer's certificate store.

Windows Update

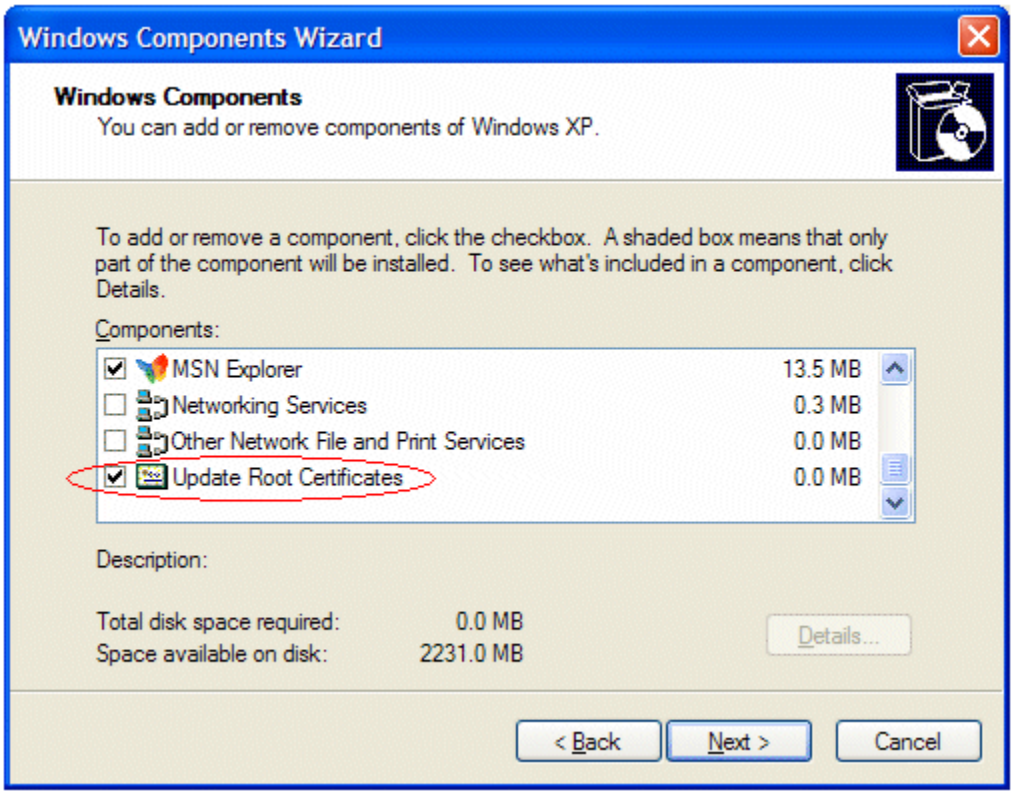
By default, computers that are running Windows XP and members of the Windows Server 2003 family run a service that will download updated public root CA certificates that have been added to the Microsoft root program. The service is not available in the Windows 2000 family.

Any organization that has a CA that meets the requirements that are outlined in the Microsoft Root Certificate program is able to distribute the CA certificate through Windows Update. For more information, see "Microsoft Root Certificate Program" on the Microsoft TechNet Web site.

Computers that are running either Windows XP or Windows Server 2003 periodically download the current list of Root CA certificates that are added to the Third-Party Root Certification Authority store on the local computer. For more information, see the chapter "Certificate support and the Update Root Certificates component" in "Using Windows XP Professional with Service Pack 1 in a Managed Environment: Controlling Communication with the Internet," which is available for download on the Microsoft Web site.

To install or remove this service, you can use **Add or Remove Programs**. To do this, click **Start**, point to **Control Panel**, and then click **Add or Remove Programs**. In the toolbar, click **Add/Remove Windows Components**, and then, in **Components**, select the **Update Root Certificates** check box.

This service can also be managed through Group Policy in Active Directory.



If your browser does not support inline frames, click here to view on a separate page.

Figure 2 Windows Components Wizard

Creating an Enrollment Strategy

A certificate can be used to provide authentication evidence of its owner, encrypt, or sign data. Because of this, the certificate issuer must ensure that certificate holders are known entities. Before certificates are enrolled, you should answer the following questions:

- How will users obtain their certificates?
- What is the process for enrollment identification?

The most secure way to initially enroll user certificates is to do a face-to-face authentication at the registration authority and store user certificates on hardware tokens. This provides the highest level of assurance, but also the highest cost of deployment.

If certificate enrollment with hardware tokens through enrollment agents is not an option, the CA can verify the certificate requester with domain credentials. This authentication method for certificate enrollment is usual when users self-enroll certificates. This scenario assumes that a user is the only person who is able to use the credentials.

It is recommended that you use a combined enrollment strategy that implements a strong initial identity check. Subsequent certificate enrollment and renewal can then be based on the initial certificate.

Creating a CA Renewal Strategy

Certificate lifetimes can have an impact on the security of your PKI for the following reasons:

- Over time, encryption keys become more vulnerable to attack. In general, the longer amount of time that a key pair is in use, the greater the risk that the key can be compromised. To mitigate this risk, you must establish the maximum allowable key lifetimes and renew certificates with new key pairs before these limits are exceeded.
- When a CA certificate expires, all subordinate certificates that are issued by this CA for validation also expire. This is known as "time nesting" and is traditionally enforced by CryptoAPI in the client.
- When a CA certificate is revoked, all certificates that have been issued by the CA must also be re-issued.

End entity certificates expire when the issuing CA certificate reaches the end of its lifetime, unless:

- The end entity certificate is renewed with a new key pair that chains to a CA certificate with a longer lifetime.
- The end entity certificate was revoked before the CA certificate expiration date is reached.

You must plan the CA certificate renewal precisely during the PKI deployment phase. If this important planning step is missed, the entire PKI might stop working when the CA certificate expires, because all of the certificates that depend on the CA's certificate are then no longer usable for both encryption and signing operations. Remember that a certificate is capable of decrypting data, even if it has expired or been revoked.

> **Note** It is strongly recommended that you generate new key material when you renew a CA's certificate in order to partition the CRL that is issued by the CA and also prevent ambiguous certificate chaining errors caused by use of the same public key.

Determining the Total Number of CAs

The total number of CAs depends on the organization's security requirements and the organization's size. It is also dependent upon the geographical, political, and business hierarchy of the organization. As outlined earlier in this document, there is a choice of different trust levels that may be applied. After the organization has decided how many tiers should be implemented, it is important to plan the number of CAs that are required at each level. For a PKI topology that uses intermediate CAs, the number of CAs depends on the number of different CA policies that are required to issue CAs. The number of issuing CAs depends on the number of certificates that should be issued, the network connectivity between the requester and the CA, and the number of intermediate CAs.

A three-tier architecture consists of:

- One root-CA
- At least one policy CA (This can be one or many servers.)
- At least two issuing CAs for every policy CA to ensure fault tolerance

A two-tier architecture consists of:

- One root-CA

- At least two issuing CAs to ensure fault tolerance
- A single-tier architecture consists only of a single CA.

Note the following:

- You cannot change the CA type at a later time; you must uninstall the original CA and then reinstall the CA to change it from either a stand-alone CA to an enterprise CA or an enterprise CA to a stand-alone CA.
- You can install only one instance of a CA on a Windows Server 2003 system.
- The certificate distribution point and the CRL publication interval is valid for all certificates that are issued by a CA and cannot be set for individual certificates.

For certificates that are used externally, the naming and information that is part of the certificates should not reveal the internal PKI or network infrastructure, such as the name of a CA or CRL distribution point paths in the issued certificates.

Hardware Requirements

This section provides some general guidelines for hardware requirements for a Windows Server 2003 CA. This section should not be used as an authoritative guide for performance characteristics. Specific performance characteristics vary, depending on the implementation and customer environment.

Hardware Guidelines

Microsoft performance testing in a lab environment has shown that the signing key length of the CA has the most significant impact on the enrollment rate of the CA. A larger number of certificates can be signed and enrolled in a given time if a smaller key size is used. If a larger key size is used, more CPU time is required to issue certificates.

The total number of issued certificates should not have a significant influence on either server performance or the rate at which the CA issues certificates; the performance of the issuing CA stays nearly the same, whether thousands or millions of certificates have previously been issued. Therefore, the scalability of the CA is considered to be linear, based on the size and performance of the disk arrays that are used to store both the database and log files.

The following table lists configuration factors that may affect performance of the CA.

Table 11 Resources That Affect CA Performance

Resource	Performance notes
Number of CPUs	Additional CPUs increase the overall performance of the CA. This is the most critical resource for a Windows Server 2003 CA.
Memory	In general, additional memory does not have a significant role in the enrollment performance of the CA. The CA should meet general recommended system requirements (512 MB), however, the minimum amount of memory is 256 MB.
Disk size	The capacity of the disk volume that stores the database and log files it the primary limiting factor for the number of certificates that a CA is able to maintain.
Disk performance	In general, a short key length (512 KB) generates very little CPU utilization and a very high disk load. Larger key sizes generate more CPU utilization and less disk usage. A high-performance disk subsystem can increase the rate of enrolled certificates. A RAID set is recommended for both performance and fault-tolerance purposes. CA operations are primarily disk-write intensive.
Number of volumes	Using separate disks for the database and log files provides basic performance improvement. In general, the drive that contains the CA database is used more than the drive that contains the log files. The disk write capacity improves if you use more physical drives in a RAID set.
RAID stripe size	It is recommended that you use a stripe size larger than 64 KB.
Key length	The larger the signature key length, the greater the CPU utilization. Larger keys degrade CA performance. To be CPU-independent, you may want to use hardware acceleration to provide a large number of both key generation and signing operations.
Bandwidth	A 100 megabit network connection is suitable to enroll a large number of certificates and causes no performance bottleneck, assuming that the server is

	running the CA exclusively with no additional applications or network services.

Processor Notes

In general, a computer that has a current processor and 512 MB of memory is considered sufficient for most organizational uses of a Windows Server 2003 CA. The enrollment rate is directly related to the ability of the CA to sign requests that are based on CPU availability. Many hardware, environmental, network, or client factors can affect the performance of a CA.

Disk Configuration Notes

Disk space and disk speed also limit the performance and scalability of a CA. Each certificate that is issued uses approximately 16 KB of disk space in the database, and an additional 4 KB is required if the private key is archived. The certificate database must contain all of the issued certificates to be able to revoke certificates and provide a record of operations. Because none of the records are ever automatically tombstoned or automatically deleted, the certificate database continuously increases in size when new certificates are issued. Nevertheless a CA administrator can use the Certutil.exe command-line utility to delete expired records from the CA database.

Scalability

The Windows 2000 CA has been tested to issue more than 7 million certificates and the Windows Server 2003 CA has been tested to issue more than 35 million certificates on a single four-processor, Intel-based computer. The maximum database size was not reached in either of the test scenarios.

Creating Certificate Policies and Certificate Practice Statements

The definition of certificate policies and the certificate practice statement (CPS) is often forgotten by technically-oriented planners. The basis for both the certificate policy and CPS are the organization's security policy.

Creating these documents is usually a joint responsibility of the legal, human resources, and information security departments.

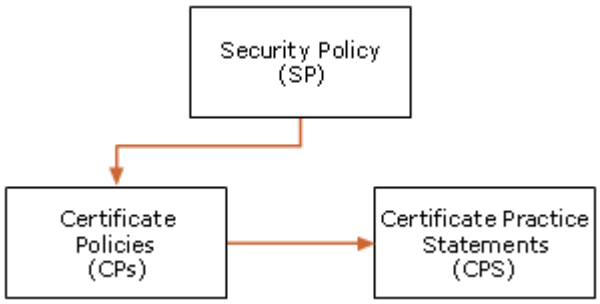


Figure 3 Relationship Between Certificate Policy and Certificate Practice Statements

Both the certificate policy and the CPS help the user of a PKI determine the level of trust that those departments can put in the certificates that are issued by a CA. The existence of policies is critical when dealing with a reliable PKI. If certificates are exchanged only within an organization, the creation of a CPS and a security policy might not be mandatory. When this is true, some clauses regarding the use of PKI and certificates in the employee manual may be essential. Note that an "organizational CPS" is a CPS that covers all CAs in a hierarchy. Generally, a CPS covers only a specific CA.

A CP and CPS may prove to required when certificate holders exchange or use certificates with partners and entities that live outside of the company's network. When external trust is implemented, it is often very important to align PKI policies and practices as part of the external contract terms.

Security Policy

The security policy is a high-level document that is created by the corporate IT group. It defines a set of rules about the use and provision of security services in the organization, and should reflect your organization's business and IT strategy. The security policy should answer high-level PKI questions, such as:

- What applications should be secured with certificates?
- What kind of security services should be offered by using certificates?

Certificate Policy

A certificate policy focuses on certificates and the CA's responsibilities regarding these certificates. It defines

certificate characteristics such as usage, enrollment and issuance procedures, as well as liability issues.

The following references define a certificate policy as a set of rules that determine if a certificate is applicable to either a community or a class of applications that have common security requirements.

For more information about the X.509 standard, see the International Telecommunication Union Web site.

For more information about the European Electronic Signature Standardization Initiative (EESSI) definition, see the EESSI Web site.

A certificate policy typically answers the question about what purposes the certificate serves, and under which policies and procedures the certificate has been issued. A certificate policy typically addresses the following issues:

- How users are authenticated during certificate enrollment
- Legal issues, such as liability, that might arise if the CA becomes compromised or is used for something other than its intended purpose
- The intended purpose of the certificate
- Private key management requirements, such as storage on smart cards or other hardware devices
- Whether the private key can be exported or archived
- Requirements for users of the certificates, including what users must do if their private keys are lost or compromised
- Requirements for certificate enrollment and renewal
- Minimum length for the public key and private key pairs

The certificate policy is typically defined by members of an organization who are known as the *policy authority*. The policy authority typically consists of representatives from different core departments, including management, legal, audit, human resources, and other departments. Overall, the policy authority members will also be members of the group that defined the security policy, which ensures that the certificate policy is in agreement with the security policy.

Certificate Practice Statement

The certificate practice statement (CPS) translates certificate policies into operational procedures on the CA level. The certificate policy focuses on a certificate; the CPS focuses on a CA. Both the EESSI and the American Bar Association (ABA) define a CPS as a statement about the way that a CA issues certificates. For more information about the ABA, see the ABA Web site. For more information about the EESSI, see the EESSI Web site.

A CPS might include the following types of information:

- Positive identification of the CA, including the CA name, server name, and Domain Name System (DNS) address
- Certificate policies that are implemented by the CA and the certificate types that are issued
- Policies, procedures, and processes for issuing, renewing, and recovering certificates
- Cryptographic algorithms, cryptographic service providers (CSPs), and the key length that is used for the CA certificate
- Physical, network, and procedural security for the CA
- The certificate lifetime of each certificate that is issued by the CA
- Policies for revoking certificates, including conditions for certificate revocation, such as employee termination and misuse of security privileges
- Policies for certificate revocation lists (CRLs), including where to locate CRL distribution points and how often CRLs are published
- A policy for renewing the CA's certificate before it expires

The CPS should be defined by a team that consists of members of the IT department, people who are operating and administering the IT infrastructure, and the people (often attorneys) that defined the certificate policy. The CPS is a public document that should be published on the Internet. Every certificate that has been issued by a CA that follows a CPS has an URL pointer in the certificate that directs people to the public document. When a certificate has a CPS pointer as part of the certificate, the **Issuer Statement** button becomes available. When you click **Issuer Statement**, the URL that has been specified by the CA administrator is redirected.

> **Important** A CPS is always valid for all certificates that are issued subordinate to the CA that contains the qualifier. Make sure that all parameters that are listed in Appendix B are part of the planning process.

Revocation Policy

Before certificates are enrolled, the PKI management team should know how to revoke certificates. Any X.509 V3 certificate (except the root CA certificate itself) should have a pointer to a valid CRL. The CRL distribution point is included in the certificate's extension and cannot be modified after a certificate is enrolled.

The logical availability of the CRL distribution point that is specified in the certificate allows a PKI-enabled application to verify the certificate's validity against the CRL. The CRL is essential to ensure the quality (status) of certificates that are published by the CA. If the CRL is available and the certificate's serial number is part of the CRL, the certificate is marked as invalid from a client's perspective.

A revoked certificate's serial number is added to the CRL as long as the original certificate lifetime is valid. After the original lifetime of the certificate expires, the serial number of the certificate is added to the CRL for the last time.

> **Note** You cannot use revoked certificates for signing or encryption operations anymore. However, you can use revoked certificates for decryption operations, because the revoked certificates are required for decryption.

If an application is going to verify a certificate against the CRL and no valid CRL is available, the revocation check does not work and the certificate cannot be used for the transaction. If the application has properly implemented CRL checking, no authentication, encryption, or signing is allowed with this certificate until a valid CRL is available again.

For immediate revocation of logon certificates, consider disabling the account in Active Directory instead of revoking the logon certificate. It is more time efficient to delete or disable user accounts if you want to immediately revoke a user's ability to gain access to the logon certificates.

For more information about CRLs, AIA, and chain building refer to the "Troubleshooting Certificate Status and Revocation" white paper on TechNet.

CRL Best Practices

When you consider CRL distribution, you should know where and how clients can gain access to a CRL. The CRL distribution mechanism of enterprise and stand-alone CAs is different by default.

It is a common mistake to not modify the default CRL distribution point of an isolated stand-alone CA. Because a root or intermediate CA is typically disconnected from the network, PKI-enabled clients cannot validate the issued certificates against the default CRL distribution point on the CA server. To make a CRL of an offline

stand-alone CA publicly available, you must manually publish the CRL or utilize a custom exit module or script that publishes the CRL to a predefined location. For more information about custom exit modules, see the "Exit Modules" chapter in the Security Platform SDK on the Microsoft Web site.

An online CA on a computer that is joined to an Active Directory domain or forest automatically publishes the CRL to Active Directory so that it can be accessible through LDAP. Alternatively, the CRL can be made available through an HTTP URL that points to a location on a Web server.

Depending on the certificate types that are issued with a CA, the order of the CRL distribution points is important. For authentication certificates, it is beneficial to have a CRL or fully-qualified LDAP CRL distribution point as the first entry in the list of distribution points. If a relative LDAP CRL distribution point is specified, a client contacts the domain controller that is closest, according to the Active Directory site structure, to get the CRL. Fully-qualified LDAP CRL distribution points eliminate latency issue that may occur until the CRL has been replicated in Active Directory. For non-authentication certificates, you may want to use LDAP because LDAP is more fault-tolerant in an Active Directory environment compared to tolerance in a single-instance HTTP server.

It is also an option to set both an LDAP and HTTP CRL distribution point URL to support clients that are Active Directory-aware, as well as clients that are not running Windows and that are not Active Directory-aware. If you have a mixed client environment or both internal and external clients, it is a best practice to place the HTTP location in the CRL distribution point extension first to avoid network timeouts. Any client that retrieves a CRL on demand during certificate verification caches a copy of the CRL in the Internet Explorer temporary files until the CRL expires..

> **Tip** It is a best practice to publish a CRL that is available externally through an HTTP location so that users and applications that are outside of the organization may perform certificate validation. It is also a best practice to use paths and naming that do not reveal the internal network infrastructure to external entities.

The CRL maintains a list of revoked certificates that have been issued by a CA. The CRL does not maintain the validity of certificates that are owned by a subordinate CA, like the CA certificate. The subordinate CA certificate's revocation status is maintained by the CA's parent CA, since the parent CA has issued the subordinate CA certificate.

Since a root CA certificate has no parent CA that could maintain the CRL, there is no need to specify a CRL distribution point for the root CA certificate itself. To revoke a root CA, all certificates that have been issued by the root CA must be revoked instead.

Here are some additional planning notes:

- A root CA certificate should have an empty CRL distribution point because the CRL distribution point is defined by the certificate issuer. Since the root's certificate issuer is the root CA, there is no value in including a CRL distribution point for the root CA. In addition, some applications may detect an invalid certificate chain if the root certificate has a CRL distribution point extension set.
- Offline CAs must continue to publish CRLs.
- If certificates are exchanged with external entities, the CRLs must be available at a location that is accessible for all internal and external entities. To satisfy this requirement, in this case the CRL is usually published in the organization's perimeter network (also known as a DMZ).
- To ensure redundancy, make the CRL available through more than one location.
- If the CRL is distributed by using Active Directory, plan for replication latency.
- Plan for CRL publications that cannot be performed as usually scheduled and have contingency operations prepared
- The CRL should be valid for the amount of time that it takes for CA recovery if hardware fails or if software does not work. For example, a one-hour CRL publication period is most likely not adequate time to perform a hardware or software restoration because of the possibility of issues with either the hardware or software.
- The more frequently that CRLs are published, the more time you will have for issue resolution.
- If a CA cannot publish the CRL on time, the CRL is not updated and will expire. If a CRL has expired, clients cannot verify certificates that would require the CRL. To prevent certificate misuse, certificates are considered invalid if the CRL has expired or is unavailable.
- A Windows Server 2003 Certification Authority can publish to an IIS cluster using UNC paths for the CRL distribution point URL.

All Windows CAs follow the CRL V2 format that is specified in RFC 2459 and RFC 3280. For additional information about RFC 2459 and RFC 3280, see the Internet Engineering Task Force Web site.

LDAP CRL Best Practices

The following best practices apply to LDAP-based CRLs:

- An LDAP CRL is replicated in Active Directory to all domain controllers in the forest. Because of this, it provides fault-tolerance in an environment with more than one domain controller and can be designated as "highly available."
- The Active Directory replication schedule should be taken into account. This is an important consideration since it may take longer than expected for every directory server to receive the latest version of the CRL, depending on the size and replication schedule of the Active Directory environment.
- CRLs should not be published to Active Directory when the CRL publication period is shorter than the replication convergence time for the Active Directory forest.
- Do not use escape characters in LDAP CRL distribution point paths, such as a backslash (\).
- Do not include names that are specific to either internal or organization names in the CRL distribution point. Certificates may be exchanged with external parties and those parties should not be able to obtain information about internal name spaces. To eliminate internal names in the CRL distribution point, also allow internal clients to gain access to the external distribution point, or implement a name mapping mechanism that ensures that internal clients can resolve an external name and gain access to an internal resource.
- If an LDAP CRL distribution point for certificates that are exchanged with external parties is used, do not use the relative LDAP URL that points to the closest domain controller.

The first part of the name is the hosting and distribution point is the LDAP name of the server that is hosting the CRL distribution point; the second part of the name is the complete LDAP path of the directory location where the CRL is stored. The following configuration string (or LDAP reference):

ldap:///CN=...,CN=...

is interpreted as

ldap://*ClosestDomainControllerBySite***/CN=...,CN=...**

When you use this syntax, part one of the LDAP CRL distribution point is left out, but it is automatically inserted when the CRL must be retrieved. The ldap:/// syntax forces a Windows 2000, Windows XP, or Windows Server 2003 client that is joined to an Active Directory domain to find the closest domain controller. Alternatively, a fully qualified domain name (FQDN) or an exact server path with a port value, is also supported.

Not only is the path of the CRL is important when you plan an LDAP CRL distribution point; you must also configure the correct search criteria and append that search criteria to the LDAP path.

LDAP searches support search suffixes to specify attributes, depth, and object-classes. Because the directory service may store several objects of different data types in the same location, it is important to query for the correct data. A search suffix uses the following format:

?attribute?depth?object_class

If the attribute, depth, and object_class search suffixes are missing, the client selects the correct object. Because there are different client implementations, a CRL verification might not work without this extended information.

The following example shows a relative LDAP CRL distribution point (on one line):

ldap:///CN=*CorporateRootCA*,CN=*Root_CA*,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,D
certificateRevocationList?base?objectClass=cRLDistributionPoint

In the sample line above, CorporateRoot, CA_*Root_CA*, *contoso*, and *com* are placeholders and must be replaced with parameters that are specific to the organization's requirements..

The following example shows an absolute LDAP CRL distribution point (on one line):

ldap://cdp1.contoso.com/CN=*CorporateRootCA*,CN=*Root_CA*,CN=CDP,CN=Public Key Services,CN=Services,C
certificateRevocationList?base?objectClass=cRLDistributionPoint

In the sample line above, *cdp1.contoso.com*, *CorporateRootCA*, *RootCA*, *contoso*, and *com* are placeholders and must be replaced with parameters that are specific to the organization's requirements..

HTTP CRL Distribution Point URL Best Practices

Non-Windows clients might not be able to retrieve CRLs with LDAP URLs based on Active Directory. Because of this, you may need to provide an additional HTTP CRL distribution point location for LDAP-enabled clients. Computers running Windows support LDAP and HTTP URLs. The following are some best practices for HTTP CRL distribution point URLs:

- If you provide an HTTP CRL distribution point location, provide fault tolerance by having either a virtual server name that points to several physical Web servers (round-robin DNS) or a clustered Web server to provide redundancy in the HTTP URL.
- HTTP CRL distribution point locations are ideal for providing accessible CRL locations for clients that are not running the Windows operating system.
- Place HTTP CRL distribution point URLs second in the list of the URLs in the CRL distribution point extension when Active Directory-aware clients are primarily used. This is to decrease network traffic because the client would benefit from intra-site communication with the domain controller.
- Place HTTP CRL distribution point URLs first in the list of the URLs in the CRL distribution point extension when clients cannot connect to the Active Directory to verify certificates. Examples include external Web servers, VPN and remote access servers, and RADIUS (IAS) servers.
- HTTP URLs should contain only valid file name characters.

Delta CRLs

In a production environment, the number of certificates that are revoked is in relation to the number of certificates that are issued. The list of revoked certificates will vary in length, depending on the number of certificates that are enrolled by a CA.

Revoked certificates are added to the CRL as a collection of certificate serial numbers. RFC 2459 and RFC 3280 define a method that you can use to reduce base CRL sizes by using delta CRLs. Delta CRLs maintain a list of certificates that have been revoked since the last base CRL publication.

Base CRLs and delta CRLs are cached by Windows clients. To ensure the validity of a certificate, the client uses the locally-cached base and delta CRL until the CRL's validity period expires. If a base CRL expires, the client retrieves a new base CRL from the distribution point that is specified in the certificate. If the base CRL is valid but the cached delta CRL is expired, a Windows client retrieves only the delta CRL. Typically, a delta CRL is much smaller in size than a base CRL because it saves only the certificates that have been revoked after the last base CRL update.

Delta CRL best practices:

- Use delta CRLs with issuing CAs whenever possible.
- Do not use delta CRLs with offline CAs, because there are not as many certificates that require frequent revocation. Offline CAs usually have longer CRL publication cycles than issuing CAs, since it is abnormal to revoke a large number of CA certificates.

To provide clients with the most up-to-date revocation information with smaller network utilization (compared

to the network utilization that is required for a base CRL distribution), you can publish the delta CRL on a daily basis and publish the base CRL on a weekly basis. However, if a large number of certificates is revoked and if the number of revoked certificates exceeds the number of revoked certificates that are already part of the base CRL, the size of a delta CRL is larger than the size of a base CRL. Note that this scenario is very unlikely to occur and is not considered to be typical.

Do not publish frequent delta CRLs to Active Directory if replication takes a longer period than the delta CRL is valid.

Online Certificate Status Protocol Support

A Windows CA does not provide online certificate status protocol (OCSP) functionality by default. However, you can enable OCSP if you install a revocation provider in CryptoAPI or through a third-party OCSP responder that communicates with the Microsoft Certification Authority. For more information about CryptoAPI or revocation providers, search for CryptoAPI on the MSDN Web site.

Best Practices for CRL Publication

The CRL publication interval for CAs that issue certificates to CAs should be a longer period than for CAs that issue certificates to end-entities, because revocation of a CA certificate should be a very rare operation. A recommended creation interval for a new CRL of that type would be in the range of 90 to 180 days.

A CRL for an offline CA should always be published a few days before expiration to allow for unexpected issues. The publication interval for issuing CAs should be set according to the type to issued certificates. Authentication certificates might require a less frequent publication schedule than other certificate types.

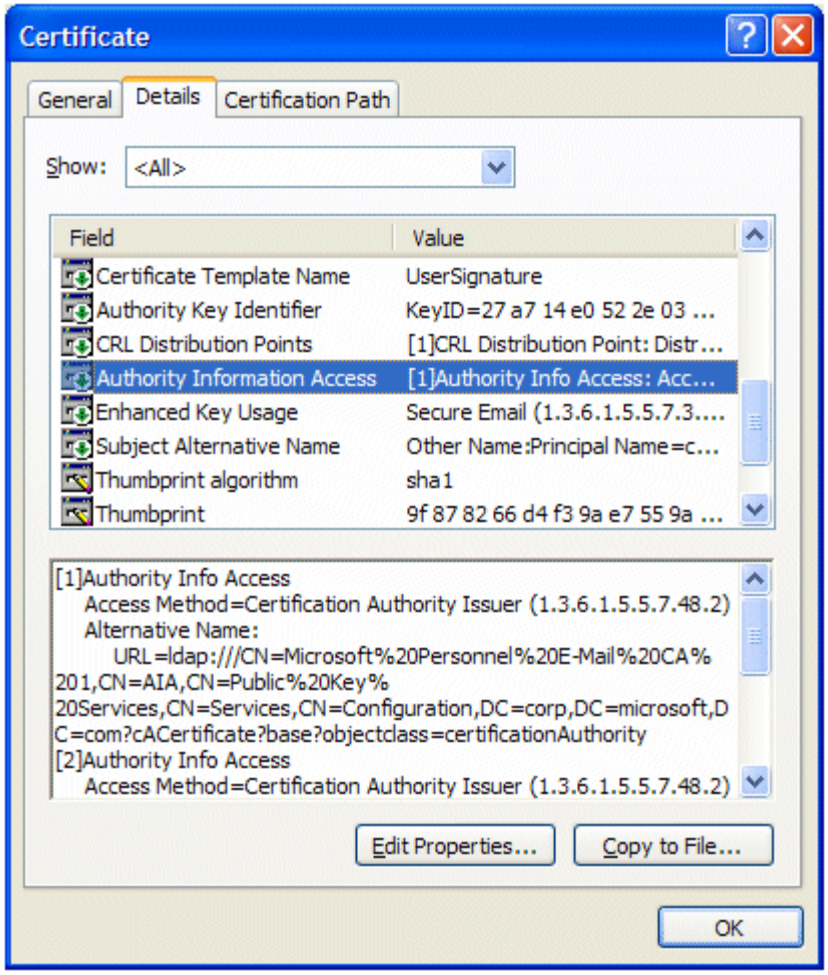
For offline CA CRL publication, you should also consider these points:

- For issuing CAs, a short CRL publishing schedule ensures that the CRL is current and that any revocation can be made available as quickly as possible. Note that Windows clients cache a CRL for the validity period.
- For offline CAs, a longer CRL publishing schedule ensures that the CRL does not have to be regenerated and republished through the required manual generation and publishing processes.

AIA Extensions

The AIA extension allows the certificate user to obtain a current copy of the CA's current certificate. CA certificates are required when a certificate chain is built. Chain building is performed as part of the certificate verification process.

When you configure AIA extensions, use the same attention to detail that you use when you configure CRL distribution point extensions. See the following example for more information about the AIA extension in a certificate.



If your browser does not support inline frames, click here to view on a separate page.

Figure 4 AIA Extensions

CA certificates are multivalued, Base64-encoded attributes in Active Directory that can store more than one CA certificate. A multivalued AIA attribute is used for every CA because a CA may have more than one valid certificate after CA renewal.

Note that multivalued attributes are limited in the number of values that they can store. You cannot sure more than 1,000 CA certificates in the AIA object.

Compared to an LDAP AIA URL that points to a multivalued object and distinguishes certificates in the same object by the search suffix, an HTTP AIA URL points only to a single file. Because of this, all HTTP URLs must include the certificate suffix (*.cer, *.crt, etc) as the suffix for the file name to distinguish between the multiple certificates that are stored in the same directory on the HTTP server

The following table describes the structure of how certificates are stored. Note that an HTTP location must be unique and only one CRL object (or file) may exist at each explicit URL path. An LDAP location is a single object in Active Directory that supports a multivalued attribute.

Table 12 Example of Stored Certificate Structure

	AIA HTTP URL (object)	**AIA LDAP URL (object)**	
Several files at http://www.microsoft.com/	concorp-ca-00_CorporateRootCA.crt concorp-ca-00_CorporateRootCA (1).crt	concorp-ca-00_CorporateRootCA.crt concorp-ca-00_CorporateRootCA (2).crt	One multivalued attribute at CN=AIA,CN=Public Key Services,CN=Services,%6%11

	concorp-ca-00_CorporateRootCA (2).crt	concorp-ca-00_CorporateRootCA (2).crt	

Certificate Validity Period and Key Length

The validity period of certificates depends on the organization's requirements. The following table outlines some recommendations for the validity period for different CA types.

Table 13 Recommendations for Validity Periods

Purpose of Certificate	Certificate Life	Private Key Renewal Strategy
Stand-alone root CA. (4096-bit key)	20 years	Renew at least every 10 years to ensure that policy CA certificates can be issued with lifetimes of 10 years. Renew by using a new key at least every 20 years.
Stand-alone policy CAs (2048-bit key)	10 years	Renew at least every 5 years to ensure that child-issuing CAs can be issued for 5 years. Renew by using a new key at least every 10 years.
Enterprise issuing CA s for medium security certificates (1204-bit key)	5 years	Renew at least every 3 years to ensure that certificates can be issued for 2 years. Renew by using a new key at least every 5 years.
Enterprise issuing CA s for high security certificates (2048-bit key)	5 years	Renew with new key at least every 4 years to ensure that certificates can be issued for a year..
Enterprise issuing CA for external certificates (1048-bit key)	5 years	Renew at least every 4 years to ensure that certificates can be issued for a year. Renew by using a new key at least every 5 years.
Secure mail and secure browser certificates	1 year	Renew by using a new key at least every 2 years.
Smart card certificates (1024-bit key)	1 year	Renew by using a new key at least every 2 years.
Administrator certificates (1024-bit key)	1 year	Renew by using a new key at least every 2 years.
Secure Web server certificates (1024-bit key)	2 years	Renew by using a new key at least every 2 years.
Business partners' user certificates for an extranet (1024-bit key)	6 months	Renew by using a new key at least every year.

Note All these values are suggestions and may be dictated by legal, governmental, or contractual rules that are specific to the organization. Changes of policy and extensions during renewal and rekey of CAs may also require subsequent changes of CPS recertification, audit, and so on.

Example Scenario for Contoso

Since a lot of planning considerations and best practice approaches are covered in the previous section, here is a real world example of PKI topology. The example describes the best practices that are mentioned earlier in this document and also describes most of the options of a complex PKI. By leaving out distinct components (like the HSM or the intermediate CA level), you can also adjust the topology to environments for smaller organizations.

The fictitious organization’s name is Contoso Company. Contoso is an international company that has already deployed Active Directory and is introducing a Windows Server 2003 PKI. The planning for the project is already finished. Besides other preparation work, the parameters as listed in Appendix B, which will drive the PKI configuration.

Use the following installation instructions to set up a PKI that is similar to the Contoso PKI.

Platform Decision

The Contoso Corporation has decided to deploy a Windows Server 2003 PKI hierarchy. The organization recognizes ease of deployment, benefits of strengthened security, security-integrated applications, and the Active Directory-integrated management infrastructure that is in their current Active Directory infrastructure.

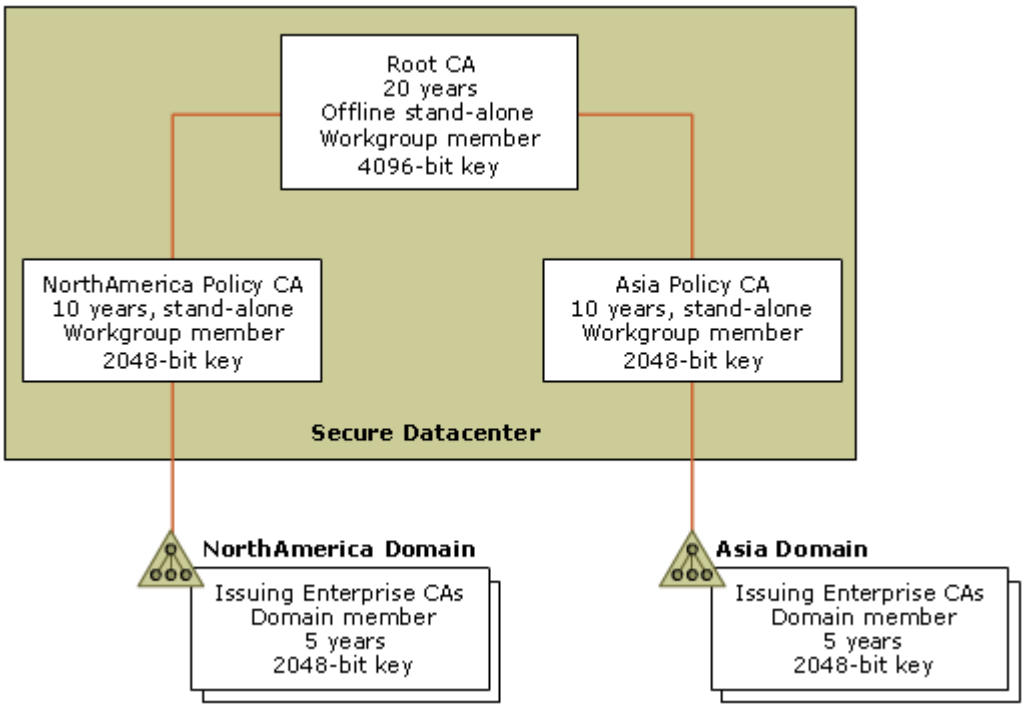
Because Contoso wants to benefit from all PKI improvements to the Windows Server 2003 family, they have prepared Active Directory to run in a Windows Server 2003 forest and in Windows Server 2003 domain functional mode. For more information about how to raise the domain functional level on a computer running a member of the Windows Server 2003 family, see the article "HOW TO: Raise the Domain Functional Level in the Windows .NET Server Family" on the Microsoft Knowledge Base.

The Contoso company has a mix of clients that are running a member of the Windows 2000 family or Windows XP Professional and uses a number of integrated applications that can take advantage of the Windows Server 2003 PKI, including Secure/Multipurpose Internet Mail Extensions (S/MIME), encrypting file system (EFS), L2TP or IPSec VPN connections, 802.1x wireless access, and SSL-enabled Web servers. Smart cards are used for user logon.

PKI Design

Contoso has decided that a three-tier PKI topology is most suitable for their organization. If an organization wants to benefit from a two-tier PKI topology, the implementation guidelines that are outlined in this documentation can also be applied.

The Contoso PKI consists of different certificate servers. Every CA will be implemented with Certificate Services as implemented in Windows Server 2003, Enterprise Edition. The following figure illustrates the Certificate Services architecture for Contoso Corporation.



If your browser does not support inline frames, click here to view on a separate page.

Figure 5 CA Hierarchy for Contoso Corporation

Root CA

The Contoso stand-alone root CA is never connected to a network and remains offline and physically secured. The root CA issues and revokes certificates for intermediate CAs in the hierarchy. To raise the security level of the CAs private key, an HSM extends the root CA's hardware configuration. The CA certificate and the CRL are manually published and made available through an HTTP and an LDAP distribution point.

Intermediate CAs

The intermediate CAs are physically secured and operated offline. Contoso has decided to operate two intermediate CAs. The separation of intermediate CAs allows the organization to set different CRL distribution points and CRL publishing intervals. Since intermediate CAs are also treated as sensitive components in the organization's PKI, they are also equipped with HSMs.

Issuing CAs

The issuing enterprise CAs are responsible for certificate enrollment to end-entities. These CAs are distributed to different geographic locations to allow local availability. Physical security, however, has to take precedence over close proximity of the servers. These CA servers are online and available to service requests at any time. You can improve availability in the future by deploying more issuing CAs.

Contoso Environment Summary

The following list describes the Contoso environment:

- A forest and domain environment with computers that run only members of the Windows Server 2003 family
- Clients that are running either Windows 2000 or Windows XP
- Three-tier PKI hierarchy
- Self-signed stand-alone offline root Windows Server 2003, Enterprise Edition stand-alone CA with HSM to support role-separation
- Intermediate offline stand-alone Windows Server 2003, Enterprise Edition stand-alone CA with HSM to support role separation
- Several online, Active Directory-integrated issuing Windows Server 2003, Enterprise Edition CAs to support auto-enrollment and V2 templates.

Stand-alone Offline Root CA

The following section describes the steps that you should use to install an offline root CA by using a computer running Windows Server 2003, Standard Edition. The installation procedure for a Windows 2000 CA is similar to the installation procedure for a computer running Windows Server 2003, Standard Edition, so you can also use the following installation procedure on computers running Windows 2000.

Note The stand-alone offline root CA is also referred to as "CorporateRootCA" in this document.

Installation Prerequisites

A server that is running Windows Server 2003, Standard Edition is installed with the base operating system and latest updates. Verify that you have the following information before you start to install Certificate Services:

- The CPS that has all of the parameters that are specific to the organization
- The Windows Server 2003 installation medium, such as the original CD-ROM
- Appropriate hardware with a floppy disk drive
- Both computer and CA naming conventions
- Directory and file paths to be used for CRL distribution point, such as AIA
- Other CA configuration information, such as CRL publication intervals
- HSM, if applicable

Install the Offline Root CA

To set up the root CA, use the steps in this section. Before you begin, verify that the following concepts have been reviewed and approved by your organization:

- Public key infrastructure concepts
- Requirements that describe the purpose of certificate usage and enrollment
- Details about CA configuration including the hierarchy of the PKI
- The renewal strategy that you are going to use for the root CA is planed
- Operational security procedures and policies

Workgroup Membership

The CorporateRootCA must be a workgroup member because it is not connected to the network and has no link to a domain controller. Nevertheless, the server name must be unique in your organization because the server name is part of the information that will be published in Active Directory.

Verify that the naming information is correct after you log on to the local computer by using the **net config workstation** command at a command prompt. (Note that the values that are in italics may be different for you, according to your configuration.) The following section is an example of how you can use the **net config workstation** command to accomplish this.

```
D:\>net config workstation
Computer name                        \\CONCORP-CA-00
Full Computer name                   concorp-ca-00
User name                            Administrator

Workstation active on
        NetbiosSmb (000000000000)
        NetBT_Tcpip_{7CD8C0C6-02A5-4EB4-8081-5D1977FD0AA5}
(0008C75BDEC0)

Software version                     Microsoft Windows Server 2003

Workstation domain                   WORKGROUP
Logon domain                         CONCORP-CA-00

COM Open Timeout (sec)               0
COM Send Count (byte)                16
COM Send Timeout (msec)              250
The command completed successfully.
```

Verify that the logon domain name is the same as your server name.

For more information, see the following articles on Microsoft Web sites:

- "Checklist: Creating a certification hierarchy with an offline root certification authority" on the Microsoft Web site
- "HOW TO: Install a Windows 2000 Certificate Services Offline Root Certificate Authority" on the Microsoft Knowledge Base

Installing an HSM on an Offline Root CA

Some organizations may choose to protect the root private key with additional hardware. Before you install and configure Certificate Services, verify that the HSM is correctly set up according to the manufacturer's installation instructions. For information about how to install an HSM on computers that are running either Windows 2000 or Windows Server 2003, see the following Web sites:

- Windows 2000 Server and PKI: Using the nCipher Hardware Security Module on the Microsoft Web site
- Deploying Certificate Services on Windows 2000 and Windows .NET Server with the Chrysalis-ITS Luna CA3 Hardware Security Module on the Microsoft Web site

Prepare the CAPolicy.inf File for the Root CA

An issued certificate typically inherits properties (for example, certificate lifetime, the distribution point of the CRL, and other parameters) from a certificate template that is provided by the issuing CA. Since the root CA requires a certificate for itself, the root CA must self-sign the root CA certificate because there is no parent CA that could issue the CA certificate.

Before the CA certificate is generated, custom configuration of the CA that is relevant to the CA certificate is required. The CAPolicy.inf file has all configuration information that is required to generate the self signed CA certificate according to the organization’s needs.

> **Warning** Configuring the CAPolicy.inf file is a very important step that you must finish before you set up a Windows Server 2003 root CA. If you do not use the CAPolicy.inf file for the offline root CA setup procedure, the CRL and AIA distribution points that become part of issued certificates are set to distribution points on the local computer. Because an offline CA is never accessible from the network, clients cannot resolve the CRL or AIA distribution point. To prevent this issue, you must explicitly add both the *CRLDistributionPoint* and *AuthorityInformationAccess* parameters to the CAPolicy.inf file. As noted in the "CRL Best Practices" section in this document, both the CRL and AIA CRL distribution point of a root CA need to be defined as “empty.”

To ensure that the CAPolicy.inf file is correctly processed:

- The ASCII text file must be available on the local computer before the CA setup procedure starts or before CA certificate renewal is attempted
- The file is placed in the **%Systemroot%** folder on the local computer on which the CA is installed

The syntax follows the specification that is described in the "CAPolicy.inf syntax" section in the appendix of this document.

Note After you use CAPolicy.inf on a CA, do not remove it from the computer because configuration parameters, like renewal key length, should be consistent during the life cycle of the CA.

Also, during the installation procedure, you do not receive a warning message if the CAPolicy.inf file is not in the correct format because there is no syntax or error-checking mechanism. For setup logging and debug information, see the *Systemroot*\Certocm.log file.

To configure the CAPolicy.inf file:

1. Log on to the CorporateRootCA computer as an administrator.
2. Open a text editor, such as Notepad.
3. Copy the sample text file that is in the "Sample CAPolicy.inf file for the CorporateRootCA" section of this document as a template.
4. Paste the text into the file and then save it to **%Systemroot%**\CAPolicy.inf.

Installing the Offline Root CA Software Components

Important Perform any renaming operations before the CA services become part of the configuration. You cannot change the NetBIOS computer name or the computer's membership in a domain or workgroup after certificate services is installed, because the name is part of the Certification Authority configuration information.

To install the offline root CA software components, use the following procedure.

1. Log on to the CorporateRootCA computer as an administrator. Note that this account will be permitted as a CA administrator during the CA installation procedure. You can delegate the CA administrator role to other user accounts after the setup and configuration procedures are finished. For more information about CA roles and permission, see Windows Server 2003 Server Help.
2. Use one of the following procedures to open **Add/Remove Windows Components**:
   a. a. To use a command prompt:
      i. Click **Start**, click **Run**, type **cmd**, and then click **OK**.
      ii. At the command prompt, type **sysocmgr /i:sysoc.inf** and then press ENTER.
   b. b. To use Control Panel:
      i. Click **Start**, point to **Settings**, and then click **Control Panel**.
      ii. Click **Add or Remove Programs**.
      iii. In **Add or Remove Programs**, click **Add/Remove Windows Components**.

   Note To run Certificate Services, check for the following software components:
   - Certificate Services
   - Internet Explorer
   - (Optional) Certificate Services Web enrollment support
   - (Optional) Internet Information Services for Web enrollment support

   It is not recommended that you install any other Windows components on a Windows Server CA. If you install additional components, reliability or security of a root CA may be compromised if a secure configuration is required by the organization.

   An offline Windows 2000 CA requires Internet Information Services to support offline CA enrollment. Unlike Windows 2000 Server, a Windows Server 2003 certification authority can process offline certificate requests within the Certification Authority MMC
3. In the Windows Components Wizard, select the **Certificate Services** check box, and then click **Next**.
4. In **CA Type**, click **Stand-alone root CA**, select the **Use custom settings to generate the key pair and CA certificate** check box, and then click **Next**.

   It is expected that the enterprise root CA and enterprise subordinate CA options are not available because the computer is not a member of an Active Directory domain.
5. Do one of the following:

- If you installed an HSM, in **CSP**, select the CSP that you installed during the HSM installation procedure.
- If you did not install an HSM, in **CSP**, click **Microsoft Strong Cryptographic Provider**.

6. In **Hash algorithm**, click the default hash algorithm, **SHA-1**.

   SHA-1 is the most common and interoperable hash algorithm that is used by applications and operating systems. For more information about CSP support on computers that are running Windows 2000, see "Microsoft Enhanced CSP Is Not Supported for Certificate Services Installations" on the Microsoft Knowledge Base.

7. In **Key length**, click **4096**.

   If you choose a different key length, confirm that the key length is interoperable with organizational applications and other PKI components. There is no verification of the key length that you type into the box. If an HSM or smart card CSP is utilized, the CSP will be required to interact with the desktop.

8. Confirm that both the **Allow this CSP to interact with the desktop** check box and the **Use an existing key** check boxes are cleared, and then click **Next**.

9. On **CA Identifying Information**, in **Common name for this CA**, type a name that will identify the CA to you. In this example, use **CorporateRootCA**.

   As it is specified in the certificate practice statement, you must specify a common name (CN) for the CA. The CN cannot exceed 64 characters in length, however, it is recommended that you use a maximum length of 51 characters to prevent an encoding length rule violation.

10. (Optional) In **Distinguished name suffix**, type **DC=concorp,DC=contoso,DC=com**.

    If you type a name, confirm that you have typed it correctly so that it works in the context of the Active Directory domain name. In the Contoso scenario, the distinguished name is **DC=concorp,DC=contoso,DC=com.** If you install a CA on a computer that is a domain member with Enterprise Administrator privileges, the distinguished name suffix is automatically configured. You can also set the distinguished name suffix at a later time by using the Certutil.exe command.

11. In **Validity period**, select **10 years**.

    Enter the validity time as defined in your organization's certificate practice statement. In this example, a validity period of 10 years is set for CorporateRootCA.

12. If you have uninstalled a CA on this computer already, you receive a warning message that confirms that you want to overwrite the private key from the previous CA installation. It is recommended that you ensure that the private key is never required again. If you make a backup copy of the system, it is more likely that you will not lose any data. (Instead of backing up the entire system, you can also make a backup copy of the private key. To do this, at a command prompt, type **certutil –backupkey -?**) If you are not sure if you want to overwrite the private key, click **No** to cancel the installation procedure. If you click **Yes**, a new key is generated and the new key replaces the existing key. Note that Windows 2000 CAs do not support the distinguished name suffix specification as part of the installation wizard.

    The public and private keys are then generated by the CSP. If you use the default CSP, the keys are written to the local computer's key store. If you did not use an HSM, the key is generated by CryptoAPI and is stored in the profile of the system account on the local computer. The length of time that is required to generate the key depends on both the size of the key that is generated and the CPU performance of the local computer. If an HSM is installed and selected, the key is generated in the HSM and stored according to the HSM specific architecture. Since no certificate templates are available on a stand-alone CA server that is a member of a workgroup, the CA certificate needs to be built from configuration information in the registry. The following default key usage extension values are added to the CA certificate:

    - Digital signature
    - Certificate signing
    - Certificate offline CRL signing
    - Certificate CRL signing

    However, if a root CA is installed on a computer that is running either a member of the Windows 2000 family or a member of the Windows Server 2003 family, and that computer is a domain member, the CA inherits the Enhanced Key Usage extension settings from the CA template in Active Directory, even if the CA is installed as a stand-alone CA. If no Active Directory is available, the Enhanced Key Usage settings are also taken out of the configuration that is available in the registry.

13. In **Certificate database** and **Certificate database log**, enter the locations of the certificate database and the log files for the certificate database.

    The certificate database and the certificate database log must be saved to a local NTFS hard disk.

On a stand-alone CA that is expected to infrequently issue CA certificates, you can retain both the certificate database and the certificate database log on the local computer's hard disk. To ensure that the CA is reliable and available, schedule backup operations of the computer. Backup may be performed even if the CA service is not running. For more information about CA backup and recovery, see "Certification Authority backup and recovery" in this document.

14. (Optional) To install a CA in the same location as a previously installed CA, select the **Preserve existing certificate database** check box.

    If you select this option, the new CA will use the existing database and preserve the certificates in the database. If you do not select this option, the existing database will be deleted. You should use this option only when you are trying to restore a CA from a backup or for CA migration.

    You can move both the database and log files to a different location. For more information, see "HOW TO: Move the Certificate Server Database and Log Files" on the Microsoft Knowledge Base.

15. Select the **Store configuration information in a shared folder** check box and, in **Shared folder**, enter a local pathname as the name for the shared folder, such as C:\CAConfig, and then click **Next**.

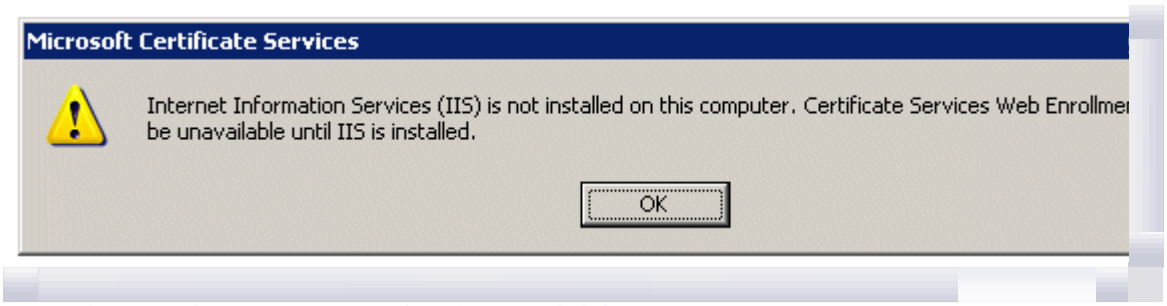
    The CA setup procedure cannot detect if the computer is supposed to run as either an online or offline CA. For an offline CA, the shared folder is not necessary, but must still be specified. If the CA is connected to the network, clients can gain access to the CA certificate through the shared folder.

    Depending on the name of the shared folder, a new share is created on the CA server computer. The path to the shared folder can be either a universal naming convention (UNC) path such as the default, \\Localhost\CAConfig, or a local path, such as C:\CAConfig. If the server does not have network cards installed or has all network interfaces disabled, you must choose a local path.

    Some information that is stored in the CA's configuration directory must be published to the organization's Active Directory at a later stage. For more information, see "Import parent CA certificates and CRLs into Active Directory" later in this document.

    When the Windows Components Wizard completes the Certificate Services configuration, you may be asked for the server's installation media to finish the installation.

    Because you do not need to install IIS on this computer, you may receive a warning message that states that the Certificate Services Web Enrollment Support is unavailable. If you receive this message, click **OK** and complete the installation procedure.



If your browser does not support inline frames, click here to view on a separate page.

Figure 6 IIS Installation Warning

Verify the Root CA Configuration

The next procedure helps you to ensure that the root CA is correctly configured ready for production operations.

Verify the Root CA Certificate

Because the CA certificate is mandatory for a reliable certificate validation of all certificates that have been issued by your PKI, it is important to ensure that this certificate has all of the necessary information before proceeding with the installation of a CA hierarchy.

1. On the local root CA computer, at a command prompt, type:

   certutil –ca.cert corporateRootCA.cer

2. View the CA certificate to validate the information that is in the CA certificate. To do this, at a command prompt, type:

   certutil.exe corporateRootCA.cer

3. Verify that the italicized parameters are the same parameters that you noted in the configuration document in the previous section. In addition, make sure that the certificate lifetime is set to a period of 10 years.

```
Signature Algorithm:
    Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA
Issuer:
    CN=CorporateRootCA

NotBefore: 6/5/2002 7:47 PM
NotAfter: 6/5/2012 7:54 PM

Subject:
    CN=CorporateRootCA
```

Verify the CorporateRootCA Configuration Information

Use the steps in this section to verify the CA configuration:

1. At a command prompt, type **certutil –cainfo** and verify the CA type. The result will be similar to the following:

   ```
   CA type: 3 -- Stand-alone Root CA
       ENUM_STANDALONE_ROOTCA -- 3
   ```

2. At a command prompt, type **certutil –getreg | find /I "Directory"** to verify the database settings. Verify the following italicized output:

   ```
   ConfigurationDirectory   REG_SZ = \\concorp-ca-00\CertConfig
   DBDirectory              REG_SZ = C:\WINDOWS\system32\CertLog
   DBLogDirectory           REG_SZ = C:\WINDOWS\system32\CertLog
   DBSystemDirectory        REG_SZ = C:\WINDOWS\system32\CertLog
   DBTempDirectory          REG_SZ = C:\WINDOWS\system32\CertLog
   ```

Offline Root CA Configuration

After the stand-alone offline root CA is installed, you must configure the properties of the offline root CA for certificates that are subsequently issued from the CA. These extensions are necessary to ensure correct revocation and chain building.

You can perform all of the steps that are described in this section by using one batch script. For more information, see "Sample script to configure CorporateRootCA" in this document.

Map the Namespace of Active Directory to an Offline CA's Registry Configuration

> **Caution** Incorrectly editing the registry may severely damage your computer. Before making changes to the registry, you should back up any valued data on the computer.

Because the offline root CA is not connected to the domain and does not automatically publish the CRL to Active Directory, you must set a key in the registry. To do this, at a command prompt, type the following command and then stop and start the CA service:

certutil.exe –setreg ca\DSConfigDN CN=Configuration,DC=concorp,DC=contoso,DC=com

where ***DC=concorp,DC=contoso,DC=com*** is the namespace of the forest root domain. This setting is primarily required for CRLs and CA certificates (AIA) that are published in Active Directory.

This registry value sets the %6 replacement token that is required for the CRL location attribute, as well as the CRL and AIA distribution points that are described in "Configure CorporateRootCA distribution points for CRL and AIA." For more information about the %6 replacement token, see "CRL distribution point replacement token" in this document.

> **Important** After you use this command to change the registry key, a new CRL and any new CA certificates that are issued must be republished. Only new certificates that are issued after you use the previous command will have this information available. It is important to note that you must reissue and republish any subordinate CA certificate if it was issued before you changed the registry key.

Configure CorporateRootCA Distribution Points for CRL and AIA

The CRL and AIA distribution points must be set before any certificates are issued from the new CA.

This configuration step ensures that the correct information is embedded in each of the issued certificates so that the certificate's signature and revocation status can be verified. For additional information about certificate status and chain building, as well as how the AIA and CRL distribution point extensions are used by CryptoAPI, see "Troubleshooting Certificate Status and Revocation" on the Microsoft TechNet Web site.

For all CA types (online or offline, root or subordinate, enterprise or stand-alone), the configuration of the AIA extension and the CRL distribution point extension is critical. If they are not configured correctly or if they contain invalid extensions, there may be unexpected problems. For example, smart card login attempts may not work, there may be invalid e-mail digital signatures, or there may be Web sites that are not trusted.

Configure CorporateRootCA Distribution Points for CRL and AIA by Using the User Interface

CRL distribution point and AIA extension changes take effect only after the CA is restarted and the extensions appear in certificates issued only after the changes are applied.

On computers that run a member of the Windows 2000 family, the CRL and AIA configuration process is different than on computers that are running a member of the Windows Server 2003 family.

Before changing the CRL configuration, verify the default settings.

Log on to the computer with an account that has Certification Authority Administrator permissions.

Type the following at a command prompt:

certutil -getreg ca\CRLPublicationURLs

The following report of the default CRL distribution points is displayed. Note these settings if you need to change the CRL configuration to its original state.

```
CRLPublicationURLs REG_MULTI_SZ =
    0: 65:C:\WINDOWS\system32\CertSrv\CertEnroll\%3%8%9.crl
    CSURL_SERVERPUBLISH -- 1
    CSURL_SERVERPUBLISHDELTA -- 40 (64)

    1: 79:ldap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10
    CSURL_SERVERPUBLISH -- 1
    CSURL_ADDTOCERTCDP -- 2
    CSURL_ADDTOFRESHESTCRL -- 4
    CSURL_ADDTOCRLCDP -- 8
    CSURL_SERVERPUBLISHDELTA -- 40 (64)

    2: 6:http://%1/CertEnroll/%3%8%9.crl
    CSURL_ADDTOCERTCDP -- 2
    CSURL_ADDTOFRESHESTCRL -- 4

    3: 0:file://\\%1\CertEnroll\%3%8%9.crl
```

As it is specified in the CPS, you must configure the CRL and AIA distribution point for certificates issued by this CA. To configure these extensions in a Windows Server 2003 CA, perform the following steps:

1. Log on to the computer running certificate services with an account that has Certification Authority Management permissions.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Certification Authority**.
3. In the console tree, right-click the name of the CA that you want to work with, and then click **Properties**.
4. Click the **Extensions** tab.

Configure CorporateRootCA Distribution Points for the CRL

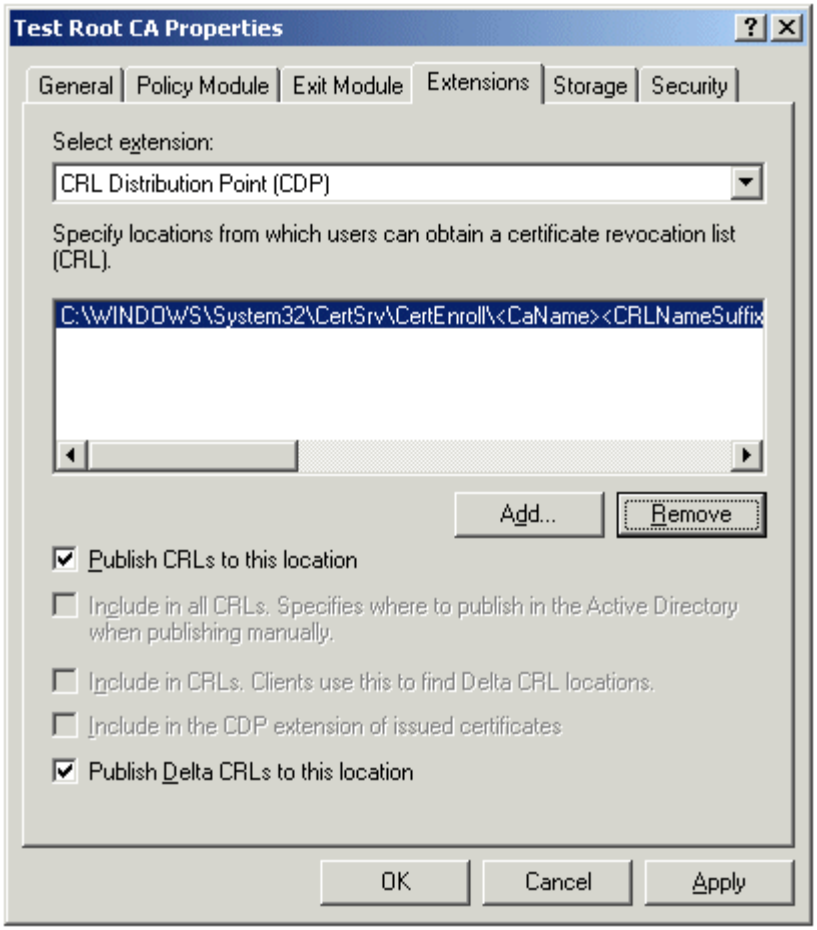
1. First, remove all of the CRL distribution point locations, except for the local CRL distribution point.

   Caution Do not remove the local CRL distribution point location**.** The local distribution point will look similar to the following path:

   C:\Windows\System32\CertSrv\CertEnroll*CorporateRootCA*.crl

   The CA must publish the CRL to the file system because all of the other distribution points are not accessible for this offline CA. The CA uses the local CRL to validate all certificates that are generated before the certificates are issued to users. The local path is not included in the CRL distribution point extension of issued certificates.
2. On the **Extensions** tab, in **Select extension**, select **CRL Distribution Point (CDP)**.
3. In **Specify location from which users can obtain a certificate revocation list (CRL)**, click the default LDAP location, click **Remove**, and then click **Yes**.
4. Repeat Step 2 for all CRL distribution point locations except for the local CRL distribution point.

After you remove all of the appropriate locations, the remaining list of CRL distribution points will be similar to the following figure.



If your browser does not support inline frames, click here to view on a separate page.

Figure 7 CRL Distribution Point Locations

Now, you will add the desired CRL distribution point locations to the list.

To provide multiple access protocol methods for CRL retrieval, different distribution points are provided to facilitate heterogeneous environments. Note that the LDAP path that is listed in the following table contains information about the organization's Active Directory namespace. If the certificate will be exchanged with external parties, define a neutral namespace. The example in this section uses the following CRL distribution points in the following order.

Table 14 List of CRL Distribution Points for CorporateRootCA

Access protocol	CRL distribution point
[local]	C:\WINDOWS\system32\CertSrv\CertEnroll\%3%8%9.crl
HTTP	http://www.contoso.com/pki/%3%8%9.crl
LDAP	Ldap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10

The [local] path should be the current Windows installation directory.

The order in which you should choose the access protocols is based on the type of certificates that are issued by a CA. A CRL distribution point with HTTP as the first protocol in the list is recommended for environments where CRL distribution without latency is critical or where most clients are not joined to an Active directory domain. HTTP locations generally do not replicate and do not have latency issues whereas an LDAP distribution point might be located in a distributed directory service, like Active Directory. The CRL distribution points that are listed in the table use the replacement tokens that are described in "CRL distribution point Replacement Token" in this document. For more information about CRL naming, see the chapter "CRL Best Practices."

1. Click **Add**, and in Location, type the appropriate CRL distribution point path from the previous table, and

then click **OK**.

You can also copy and paste the path from the table.

2. Repeat Step 1 for each type of access protocol.

Next, you must set the configuration parameters that dictate how the CRL will be published by the CA. The properties must be set for every CRL distribution point path.

3. In **Specify locations from which users can obtain a certificate revocation list (CRL)**, click one of the paths.
4. While still on the **Properties** tab, select or clear the check box that is listed in the previous table, depending on the type of path, and then click **Apply**.
5. Repeat steps 3 and 4 for each path.

Table 15 CRL Distribution Point Properties

CRL distribution point property	File	HTTP	LDAP
Publish CRLs to this location check box	Select	N/A	Clear
Include in all CRLs check box	N/A	N/A	Select
Include in CRLs check box	N/A	Clear	Select
Include in the CDP extension of issued certificates check box	N/A	Select	Select
Publish delta CRLs to this location check box	Clear	N/A	Clear

Notes

- In **Publish CRLs to this location**, since the *CorporateRootCA* computer is not attached to the network, the CA cannot automatically publish the CRL to the LDAP CRL distribution point. By default, this option is chosen on an enterprise CA to automate the CRL publishing to the LDAP CRL distribution point.
- In **Publish CRLs to this location**, a UNC file path can be specified to publish to clustered Web servers using IIS for CRL fault tolerance.
- If the **Publish Delta CRLs to this location** check box is selected, make sure that the delta CRL is also published. For more information, see "Configure CRL publication interval via the user interface" in this document.

For a description of CRL properties, see "CRL publishing properties" in this document.

Configure CorporateRootCA Distribution Points for AIA

Caution In the procedure below, do not remove the local AIA path location**.** The local path will not be contained in the AIA extension of issued certificates.

1. In *CorporateRootCA* **Properties**, on the **Extensions** tab, select **Authority Information Access (AIA)**.
2. **In Specify locations from which users can obtain the certificate for this CA**, click the default LDAP location, click **Remove**, and then click **Yes**.
3. Repeat the previous step to remove all of the entries except for the local entry.

You can also clear the check boxes for all AIA publishing options instead of removing the AIA path from the list.

4. Click **Add**, and in **Location**, type one of the AIA distribution points from the following table, and then click **OK**.
5. Repeat the previous step for each AIA distribution point in the table below.

Note that the LDAP path can expose internal namespace information if the certificates will be exchanged with external parties. Change the LDAP CRL distribution point to a permanent and publicly-available distribution point if certificates are exchanged with external parties.

Table 16 List of AIA CRL Distribution Points for Contoso

Access protocol	AIA Distribution Point
[local]	D:\WINDOWS\system32\CertSrv\CertEnroll\%1_%3%4.crt
HTTP	http://www.contoso.com/pki/%1_%3%4.crt

LDAP	ldap:///CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11

6. In **Specify locations from which users can obtain the certificate for this CA**, click one of the locations, and then select or clear the check boxes according to the following table.

   These configuration parameters control how the AIA extension is used by the CA in issued certificates. You must set the properties for every AIA path that is specified on the **Extensions** tab.

   Table 17 AIA Properties

AIA property	FILE	HTTP	LDAP
Include in the AIA extension of issued certificates check box	N/A	Select	Select
Include in the online certificate status protocol (OCSP) extension check box	N/A	Clear	Clear

7. Repeat the previous step for each location, except for the file locations.
8. Click **OK**, and then click **Yes** to apply the changes you have made and restart the computer.

Configure the *CorporateRootCA* CRL and AIA CRL Distribution Point From a Batch File

The CRL distribution point path is stored as a multivalued attribute in the registry. You can also set the appropriate value with the Certutil.exe utility. This procedure is similar to the steps that are outlined in "Configure CorporateRootCA distribution points for CRL and AIA by using the user interface" earlier in this document. To configure both the CRL distribution point and AIA paths for a Windows Server 2003 CA with **Certutil.exe**, follow the steps that are described in this section.

> **Important** Because percent character (%) variables are handled differently than the configuration UI in batch files and at a command prompt, you must use the %% notation if you want to run the example script in this section as a batch file. If Certutil is called from a command prompt, replace %% with a single %.

Certutil.exe interprets a multivalued attribute when you use **\n** as part of the value string. If a multivalued attribute consists of only one value, verify that **\n** is appended as the last character in the value string. Otherwise, you create a string value that might be not recognized by the CA. For more information, type **certutil.exe –setreg -?** at a command prompt.

1. On a server that is running one of the appropriate members of the Windows Server 2003 family, open a text editor, such as Notepad, and then copy the following text as two separate rows into the text editor.

```
certutil -setreg CA\CRLPublicationURLs
"1:%WINDIR%\system32\CertSrv\CertEnroll\%%3%%8%%9.crl\n2:http://www.
contoso.com/pki/%%3%%8%%9.crl\n10:LDAP:///CN=%%7%%8,CN=%%2,CN=CDP,CN
=Public Key Services,CN=Services,%%6%%10"
certutil -setreg CA\CACertPublicationURLs
"1:%WINDIR%\system32\CertSrv\CertEnroll\%%1_%%3%%4.crt\n2:LDAP:///CN
=%%7,CN=AIA,CN=Public Key Services,CN=Services,%%6%%11\n2:http://www
.contoso.com/pki/%%1_%%3%%4.crt"
```

   If a Windows 2000 Server is used, the following commands perform the same function as above:

```
certutil -setreg policy\RevocationCRLURL
"http://www.contoso.com/pki/%%3%%8.crl\n"

certutil -setreg policy\LDAPRevocationCRLURL
"ldap:///CN=%%7%%8,CN=%%2,CN=CDP,CN=Public Key
Services,CN=Services,%%6?certificateRevocationList?base?objectclass=
cRLDistributionPoint\n"
certutil -setreg policy\FileRevocationCRLURL "\n"

certutil -setreg policy\IssuercertURL
"http://www.contoso.com/%%1_%%3%%4.crt\n"
certutil -setreg policy\LDAPIssuercertURL
"ldap:///CN=%%7,CN=AIA,CN=Public Key
Services,CN=Services,%%6?cACertificate?base?objectclass=
certificationAuthority\n"
certutil -setreg policy\FileIssuercertURL "\n"
```

2. Save the text file as **%temp%\MyCRLCDP.cmd**.
3. Close the text editor.
4. At a command prompt, type **%temp%\MyCRLCDP.cmd** to execute the commands from the text file.

5. At a command prompt, type **net stop certsvc** to stop the certificate server, because you must restart the computer to apply the change.
6. At a command prompt, type **net start certsvc** to restart the certificate server.

Verify the CorporateRootCA CRL and AIA Configuration

Because the configuration of CRL and AIA distribution points is very important, verify your configuration:

1. Do one of the following:

If your CA is running	Do this
A member of the Windows 2000 Server family	At a command prompt, type the following commands, pressing ENTER after each line: **certutil –getreg policy\RevocationCRLURL** **certutil –getreg policy\LDAPRevocationCRLURL** **certutil –getreg policy\FileRevocationCRLURL**
A member of the Windows 2003 Server family	At a command prompt, type the following command, and press ENTER: **certutil –getreg ca\CRLPublicationURLs**

2. Verify that the output is similar to the values you have configured in the previous section.
3. Do one of the following:

If your CA is running	Do this
A member of the Windows 2000 Server family	At a command prompt, type the following commands, pressing ENTER after each line: **certutil –getreg policy\IssuerCertURL** **certutil –getreg policy\LDAPIssuerCertURL** **certutil –getreg policy\FileIssuerCertURL**
A member of the Windows 2003 Server family	At a command prompt, type the following commands, pressing ENTER after each line: **certutil –getreg ca\CACertPublicationURLs**

4. Verify that the output resembles the following output and contains the proper organizational naming information.

```
  CACertPublicationURLs REG_MULTI_SZ =
    0: 1:D:\WINDOWS\system32\CertSrv\CertEnroll\%1_%3%4.crt
    CSURL_SERVERPUBLISH -- 1

    1: 2:ldap:///CN=%7,CN=AIA,CN=Public Key
Services,CN=Services,%6%11
    CSURL_ADDTOCERTCDP -- 2

    2: 2:http://www.contoso.com/pki/%1_%3%4.crt
    CSURL_ADDTOCERTCDP -- 2
```

Configure CRL Publication Interval By Using the User Interface

After the CRL distribution point is set, you must configure the CRL publication interval. To configure the publication schedule, use the following procedure.

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Certification Authority**.

   This opens the Certification Authority MMC Snap-in.
2. In the console tree, right-click **Revoked Certificates**, and then click **Properties**.
3. In CRL publication interval, type a number for the CRL publication interval according to your CPS.

   For planning information, see "Best practices for CRL publication" in this document. Note that publishing by using minute-based intervals is available only through the registry and is not recommended for most installations.
4. Verify that the **Publish Delta CRLs** check box is not selected.

   The **Publish Delta CRLs** setting is not available on computers running a Windows 2000 CA.

Configure CRL Publication From a Batch File

You can configure the CRL publication schedule information in the registry by using the **Certutil.exe** utility. To configure the CRL publication schedule information by using **Certutil.exe**, use the steps in this section. Note that this configuration script works on a Windows 2000 CA, except for the **CRLDeltaPeriodUnits** configuration.

1. Start a text editor, such as Notepad, and then copy the following text into a text file:

```
certutil -setreg CA\CRLPeriodUnits 180
certutil -setreg CA\CRLPeriod "Days"

certutil -setreg CA\CRLDeltaPeriodUnits 0

net stop certsvc & net start certsvc
```

2. Save the text file as **%temp%\MyCRLPeriod.cmd**, and then close the text editor.
3. At a command prompt, type **%temp%\ MyCRLPeriod.cmd**, and then press ENTER.

Set the Validity Period for Issued Certificates at the Offline Root CA

The lifetime of certificates that are issued by a Windows stand-alone CA is set to one year by default. Because these values might not match the organization's requirements, you must set a registry key to adjust this default value.

The settings are valid for both a Windows Server 2003 CA and a Windows 2000 CA.

Note The validity time of the root CA certificate is controlled at the setup and renewal of the CA certificate through the value that is specified in the CAPolicy.inf file. The registry value that is described in this section does not affect the validity time of the root certificate.

1. Start a text editor, such as Notepad, and then copy the following to a text file:

```
certutil -setreg ca\ValidityPeriodUnits 10
certutil -setreg ca\ValidityPeriod "Years"
net stop certsvc & net start certsvc
```

2. Save the text file as **%temp%\MyVP.cmd**, and then close the text editor.
3. At a command prompt, type **%temp%\MyVP.cmd**.

For more information on allowing certificate requests to control the certificate validity time, see "Control certificate validity time by certificate request" in this document.

For more information about how to change the expiration date of certificates that are issued by a Windows 2000 CA, see "HOW TO: Change the Expiration Date of Certificates Issued by a Windows 2000 Certificate Authority" in the Microsoft Knowledge Base.

Republish the CorporateRootCA CRL

After the CRL distribution point extensions are updated on the CA, new CRLs must be published to ensure that all of the clients will be able to gain access to the most current revocation list information. The publishing can be done through the MMC or by using **Certutil.exe** at a command prompt with the same results.

Republish the CRL by Using the MMC

Use the steps in this section on either a Windows Server 2003 CA or a Windows 2000 CA to republish the CRL. It is important to republish the CRL because adapted configuration parameters such as **DSConfigDN** are included as attributes in the CRL. Also, CRL properties affect the publication of the CRL.

1. Log onto the CA server with CA Manager permissions.
2. Open the Certification Authority MMC. To do this, click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Certification Authority**.
3. Right-click **Revoked Certificates**, point to **All Tasks**, and then click **Publish**.

   A new base CRL is published. A delta CRL is published only if you have also set the CRL delta publication schedule.
4. When you are prompted to confirm the type of CRL that should be published with this request, click **New CRL**.

   Because only base CRLs are published by the offline root CA, only the **New CRL** option is available.

Republish the CRL from a Command Prompt

To publish the CRL, at a command prompt, type **certutil -CRL**, and then press ENTER. When you do this, the CRL is published to the location that you configured.

Verify the Published CRL

There are two attributes that you should verify after the CRL is published: the publication time and the **Published CRL locations** attribute. When you verify the publication time for the CRL, you are also verifying whether the correct CRL publication is set on the configured schedule. You also need to verify that the **DSConfigDN** registry value is set correctly and that the **DSConfigDN** registry value is in the CRL.

Determine the Name of the Most Current CRL

1. At a command prompt, type **certutil –dynamicfilelist**, and note that the CRL path name that is displayed.
2. At a command prompt, type **certutil**, and use the CRL path and file name from the previous step as the command-line parameter. For example, you can type the following:

   certutil %systemroot%\System32\CertSrv\CertEnroll*CorporateRootCA.crl*

   where *CorporateRootCA.crl* is the file name of the current CRL.
3. Verify that the **Effective date** attribute has the same time as the expected CRL publishing time.
4. Verify that the **Published CRL Locations** attribute does not have a DC=UnavailableConfigDN namespace.

   The **Published CRL Locations** attribute is used to verify the original location of the CRL's publication. If the namespace is set to **UnavailableConfigDN**, clients will report an error because the CRL's original distribution point cannot be verified.

```
Published CRL Locations
 [1]Locations
  Distribution Point Name:
   Full Name:
    URL=ldap:///CN=CorporateRootCA,CN=concorp-ca-
00,CN=CDP,CN=Public%20Key%20Services,CN=Services,DC=Unavailable
ConfigDN?certificateRevocationList?base?objectClass=cRLDistributionPoint
```

If the output has a **DC=UnavailableConfigDN**, to resolve this behavior, see "Map the namespace of Active Directory" or "Republish the CorporateRootCA CRL," earlier in this document.

A CRL that is correctly configured should have the following output:

```
Published CRL Locations
 [1]Locations
  Distribution Point Name:
   Full Name:
     URL=ldap:///CN=CorporateRootCA,CN=concorp-ca-00,CN=CDP,CN
=Public%20Key%20Services,CN=Services,CN=Configuration,DC=concorp,
DC=contoso,DC=c
om?certificateRevocationList?base?objectClass=cRLDistributionPoint
```

Caution Verify that the italicized text is the same as the value that is specified in **DSConfigDN** registry values. You should also verify that **objectClass** component of the LDAP path is correctly defined.

Finalize the CA Configuration

If you use the steps in the previous sections, the CA is operational and ready to issue certificates.

If you install a Windows 2000 CA instead of a Windows Server 2003 CA, it is recommended that you also apply the additional configuration steps that are explained in "Disable issuer name and issuer serial number," later in this document.

Stand-alone Offline Intermediate CA (IntermediateCA1)

The stand-alone offline intermediate CA is also described as IntermediateCA1 in this document.

An offline stand-alone intermediate CA is part of a three-tier topology and is primarily used to add another layer of flexibility in an organization. The IntermediateCA1 is required to issue certificates to enterprise CAs that enroll authentication certificates only according to the CPS.

If you plan to implement a two-tier topology, skip this section and go to "Online Enterprise Issuing CAs (CorporateEnt1CA)," later in this paper.

Installation Prerequisites

To correctly install and configure the offline stand-alone intermediate CA, you will need the following:

- The CPS that has all of the parameters that are specific to your organization. For more information, see

"Certificate practice statement," earlier in this paper.

- The Windows Server 2003 Server installation media
- Appropriate hardware with a floppy disk drive
- Two floppy disks, one labeled **Transfer-RootCA** and the second labeled **Transfer-IntermediateCA**.

For more information about how to configure a Windows 2000 CA, see the Microsoft Web site.

The IntermediateCA1 must be a workgroup member because it is not connected with the network and has no connectivity to a domain controller. It is also important to ensure that the computer name of this server is unique in the organization's network, because the computer name is part of the CA configuration information that is published in Active Directory (For more information, see "Import Parent CA Certificates and CRLs into Active Directory" later in this document.) To ensure that the computer is a workgroup member, log on to the computer that becomes the offline intermediate CA and type the following at a command prompt, and then press ENTER:

net config workstation

If necessary, change the domain membership to a workgroup membership.

Install an HSM on IntermediateCA1

Before the CA setup procedure starts, verify that the Hardware Security Module (HSM) is set up correctly, according to the manufacturer's installation guide. For more information, see "Installing an HSM on an offline root CA" in this document.

Prepare the CAPolicy.inf File for IntermediateCA1

You must provide a CAPolicy.inf file before the CA setup procedure. The most important aspect of the capolicy.inf procedure is to allow all issuance policies at the intermediate level. A root CA always issues a SubCA certificate with all issuance policies allowed. At the intermediate CA level, this attribute must be set explicitly, otherwise it would allow all application policies but no issuing policies. An issuing CA cannot define any issuing policy if the CA certificate does not permit issuing of certificates. For more information, see Chapter 4.2.1.5, "Certificate Policies" at the Internet FAQ Archives Web site.

A stand-alone CA cannot define policies by certificate templates, because this is a feature of customizable V2 templates. A stand-alone CA does not benefit from V2 templates to issue certificates. The CAPolicy.inf file defines the policy that applies to all certificates that are issued by the intermediate CA.

Compared with the CorporateRootCA configuration, the CAPolicy.inf file does not need predefined CRL and AIA extensions because these configuration attributes are inherited from the parent CA which issues the subordinate CA certificate. Remember, that there are prerequisites that a CAPolicy.inf file gets processed properly.

Perform the following steps:

1. Log on to the IntermediateCA1 computer with administrative privileges.
2. Use a text editor, such as Notepad, to prepare the CAPolicy.inf file. For a template, use the sample file that is in "Sample CAPolicy.inf file for the IntermediateCA1" later in this paper.
3. Save the file to **%systemroot%\CAPolicy.inf**

Obtain the Certificate and Its CRL from CorporateRootCA

Before you can set up the IntermediateCA1 computer, you must install the root CA certificate and the most current CRL that CorporateRootCA provides, because IntermediateCA1 verifies the root certificate trust during installation.

You may need to manually obtain the parent CA's certificate once. After the parent CA has been renewed, a new CA certificate must be imported into the IntermediateCA1 certificate store again. Because the root CA and the intermediate CA are not normally connected to the network and are offline, you cannot make the root CA certificate available via the network to the intermediate CA.

Compared to the CA certificate that can have a long validity time, such as several years, the importing method that you use for the offline parent CA CRL must be performed at regular intervals that correspond to the CRL publication interval. (For more information, see "Configure CRL publication interval by using the user interface," earlier in this paper.) You have to import the offline parent CA CRL regularly because an offline CA cannot retrieve CRLs automatically through the network. You must install a copy of the latest CRL in the local certificate store of an offline CA.

The CRL and the CA certificate are transferred to the subordinate CA computer on a floppy disk in the following configuration steps. The certificate and the CRL are available in a file format on the computer that is running as CorporateRootCA.

To retrieve the CA certificate and CRL:

1. Log on to the computer that is running the CorporateRootCA as a user.
2. At a command prompt, type the following command to copy the current certificate to the Transfer-RootCA floppy disk:

   certutil –ca.cert a:\concorp-ca-00_*CorporateRootCA***.crtc > nul**

   Note If the CA has already been renewed, there might be more than one CA certificate available. In that case, use the **copy** command to transfer all CA certificates from the file system to the floppy disk. To do this, at a command prompt, type the following and press ENTER.

   copy %systemroot%\system32\certsrv\certenroll*.crt a:\.
3. To copy the CRL to a floppy disk, at a command prompt, type :

   certutil -GetCRL a:*CorporateRootCA***.crl**
4. Remove the **Transfer-RootCA** floppy disk from the drive, and then insert the floppy disk into the subordinate CA computer.

   Note If the certificate was already renewed, there may be more than one CRL, so it is safest to copy all of the available CRLs from the *Systemroot*\System32\CertSrv\CertEnroll folder to the disk. However, during initial setup of the root CA, there should be only one CRL in the directory. If a .crl file has a + sign at the end of its name, the **Publish Delta CRLs** option has not been switched off, as explained in an earlier configuration step.

You can also export a certificate through the Certification Authority MMC snap-in. For more information about how to do this, see "Export the offline intermediate certificate at the root CA" in this document.

Import the Root CA Certificate and CRL to the Intermediate CA

The root CA certificate is required during the installation of the intermediate CA. It must be installed in the intermediate CAs certificate store before the intermediate CA is set up. Use the Certutil.exe command to import CA certificates into the certificate store, as described later in this section. When you do this, the certificates and CRLs are imported in the correct location.

If the *CorporateRootCA* certificate has been renewed, it is important that you import the entire set of CA certificates and CRLs. A set can be identified by the version number, because the CA certificate and CRL have the same version number.

Example

If *CorporateRootCA* is running with a certificate that was generated during installation, then the following files must be imported into the intermediate CA.

Table 18 Files to Import With a New Certificate

File name	Description
Concorp-ca-00_CorporateRootCA.crt	CA certificate
CorporateRootCA.crl	CRL

As mentioned earlier, you must import the CA certificate and CRL from the *CorporateRootCA* after the Root CA certificate was renewed. In the example below, note that Windows adds an incremental value to the filename if there is more than one CA certificate and CRL. For example, if the *CorporateRootCA* has been renewed twice, you must import the following list of files into IntermediateCA1.

Table 19 Files to Import With a Previously-Used Certificate

File name	Description
Concorp-ca-00_CorporateRootCA(2).crt	CA certificate
CorporateRootCA(2).crl	CRL

Import the Root CA Certificate and CRL to an Intermediate CA Using the MMC

This section describes how you can import a certificate import by using the Certificates MMC. The following steps about how to import the root CA and CRL to an intermediate CA by using the MMC snap-in are primarily for illustration purposes.

It is easier to import the CA certificates at a command prompt. The procedure for this is given later in this section.

1. To use the Certificates MMC to import a certificate and CRL, first verify that the CA certificate uses both the correct context and container. Log on to the IntermediateCA1 computer as a local administrator. Local admin permissions are required to import certificates or CRL's into the local systems' certificate store.
2. Click **Start**, click **Run**, type **mmc.exe**, and then press ENTER.
3. Add the Certificates MMC snap-in:
   a. On the **File** menu, click **Add/Remove Snap-in**, and then click **Add**.
   b. Click **Certificates**, and then click **Add**.
   c. Click **Computer account**, and then click **Next**.
   d. Click **Local computer**, and then click **Finish**.

      Note Because there are different certificate stores on a computer, you must select the correct certificate store. The computer account is required because the CA runs as part of the local system security context. Because of this, the CA can gain access to all of the information that is stored in the local computer's certificate store. Only security principals who have administrative permissions on the computer can write certificates to the System certificate store.

      For detailed description about certificate stores, see the Security chapter of the Windows 2000 Resource Kit on the Microsoft Web site.
   e. Click **Close**, and then click **OK**.
4. Import the certificate. To do this:
   a. Click **Certificates**, and then, on the **View** menu**,** click **Options**.
   b. Select the **Physical certificate stores** check box.
   c. In the console tree, double-click **Certificates (Local Computer)**, double-click **Trusted Root Certification Authorities**, and then double-click **Registry**.
   d. Right-click **Certificates**, point to **All Tasks**, click **Import**, and then click **Next**.
   e. Insert the **Transfer-RootCA** floppy disk into the floppy disk drive, and then click **Browse**.
   f. Navigate to the certificate file, and then click **Open**.
   g. Decide the location where you want the certificate stored, click **Place all certificates in the following store**, and then click **Next**.

      Note that your current certificate container is the predefined value because the import procedure has been started from there.
   h. After you view the report about which options you selected in the import wizard, click **Finish** to import the certificate.
   i. After you click **Finish**, you receive a message that confirms the status of operations. Also, the certificate appears in the list of certificates.
5. Import the CRL. To do this:
   a. Double-click **Certificates (Local Computer)**, and then double-click **Trusted Root Certification Authorities**.
   b. Right-click **Registry**, point to **All Tasks**, click **Import**, and then click **Next**.
   c. Insert the **Transfer-RootCA** floppy disk into the floppy disk drive, and then click **Browse**.
   d. Browse to your floppy disk drive, click the CRL file, and then click **Open**.
   e. Click **Place all certificates in the following store to decide in which location the certificate should be stored**, and then click **Next**.

      The registry node that is under Intermediate Certification Authorities is the predefined value because the import procedure has started as an action on the Intermediate Certification Authorities container.
   f. After you review the report that displays the options that you have selected, click Finish to import the certificate.

After you complete this procedure, the CA certificate and the CRL are installed in the local computer's certificate store.

Note You must repeat the steps in this section to import more CRLs and certificates. You must do this if the CorporateRootCA certificate has been renewed or a new version of the CRL has been published.

Find a Certificate in the Certificate Store

If you imported the certificate into the incorrect certificate store, you may want to use the Find Certificates option.

You can also use the **Find Certificates** option to identify duplicate certificates that exist in several certificate stores. If you correctly set up the certificate, the certificate is kept only one time. If the same certificate appears several times, remove the duplicate certificates and verify that the certificate is stored in the correct container. It is important to know which certificate belongs in which certificate store. For information about how to verify CA certificates, see the "Relationship of the Configuration Container and Certificate Store" section in this document. For more information regarding root certificates, see the articles "Trusted Root Certificates That Are Required By Windows 2000" on the Microsoft Web site and "How to Remove a Root Certificate from the Trusted Root Store" on the Microsoft Knowledge Base.

To find a certificate in the certificate store:

1. Click **Start**, click **Run**, type **mmc.exe**, and then press ENTER.
2. Right-click **Certificates**, and then click **Find Certificates**.
3. Choose your search criteria, and then click **Find Now**.

If your search is successful, you will see a list of certificates and the certificate's corresponding store that match your search criteria.

Import the Root CA Certificate and CRL into an Intermediate CA from a Batch File

To import both the root CA certificate and the CRL from a batch file:

1. Log on to the IntermediateCA1 computer as a local administrator because local administrative permissions are required to import certificates or CRLs into the local computer's certificate store.
2. Click **Start**, click **Run**, in the **Open** box, type **cmd.exe**, and then press ENTER.
3. Insert the floppy disk labeled **Transfer-RootCA** into the floppy disk drive on the intermediate CA computer.
4. At a command prompt, type the following two commands, and then press ENTER.

   for %C in (*FloppyDrive***:*.crt) do certutil –addstore –f Root %C**

   for %C in (*FloppyDrive***:*.crl) do certutil –addstore –f Root %C**

   where *FloppyDrive* is the drive letter of the floppy disk drive.

This will install all certificates and the latest CRL to the appropriate CryptoAPI store. (Note that the loop around the **certutil** command simplifies the import procedure because there may be more than one certificate or CRL on the floppy disk that needs to be imported.) The optional **–f** parameter forces an overwrite of the certificate if the certificate has been previously added to the store.

Only valid certificates are imported to the certificate store.

> **Note** Because it might be difficult to determine which CA certificate or CRL version is required, it is recommended that, if several CRLs exist, you import all CRLs from the root CA. For more information about the CA certificate and CRL storage, see "Relationship of the configuration container and certificate store" in this white paper.

Verify the Root CA Certificate Import Procedure From a Command Prompt

After both the root CA certificate and CRL are imported, you can use the **Certutil.exe** utility to confirm that the import procedure was successful. It is important to insure that the certificates have been put into the right certificate stores.

To see a list of certificates that are stored in the root CA certificate store, type the following command at a command prompt:

certutil –verifystore root

The version number is shown as part of the output text that will appear. Confirm that the version number of the CA certificate and the CRL match..

Install the Offline Intermediate CA Software Components

The installation procedure that you use for a subordinate CA is different from the installation procedure that you use for a root CA. Use the following steps to set up IntermediateCA1:

1. Log onto IntermediateCA1 as a local administrator.

   During the CA installation procedure, this account becomes a CA administrator, which is a role that can also be delegated to other user accounts. For more information about CA roles and permission, see Windows Server 2003 Server Help.

2. To open the Windows Components Wizard, do one of the following:

To	Do this
Use a command prompt	1. Click **Start**, click **Run**, and in **Open**, type **cmd**, and then click **OK**. 2. At the command prompt, type **sysocmgr /i:sysoc.inf**, and then press ENTER.
Use Control Panel	1. Click **Start**, point to **Settings**, point to **Control Panel**, and then click **Add or Remove Programs**. 2. In **Add or Remove Programs**, click **Add/Remove Windows Components**.

3. Select the **Certificate Services** check box, and then click **Next**.

   To correctly run Certificate Services, the following list of software components is required. Web enrollment and IIS are optional components on an offline Windows Server 2003 CA that could be installed with the CA at the same time or at a later date.

   Note As described in "Installing the offline root CA software components" in this document, IIS is not required on an offline CA. However, you can have IIS on the computer in order to enroll certificates through Web enrollment support. IIS is not recommended as a security best practice, but is shown in this document only as an example for the procedures.

   Certificate Services

   - Certificate Services CA
   - Certificate Services Web enrollment support

   Internet Explorer

   Application Server

   - Enable network COM+ access
   - Internet Information Services (IIS)
   - Common Files
   - Internet Information Services Manager
   - World Wide Web services
   - Active Server Pages
   - World Wide Web services

   A Windows 2000 offline CA requires IIS in order to satisfy offline requests. A Windows Server 2003 CA is also able to process offline certificate requests as a function of the Certification Authority MMC. Alternatively, you can submit offline requests from a command prompt by using **Certreq.exe**.

4. When you are prompted to choose the type of installation procedure, click **Stand-alone subordinate CA,** select the **Use custom setting to generate the key pair and CA certificates** check box, and then click **Next**.

   The **Enterprise Root CA** and **Enterprise Subordinate CA** options are not available because the computer is not a member of an Active Directory domain.

5. Do one of the following:

   - If you installed an HSM, in **CSP**, you must select the CSP that you installed during the HSM installation procedure in **CSP**.
   - If you did not install an HSM, in **CSP**, click **Microsoft Strong Cryptographic Provider**.

6. In **Hash algorithm**, click **SHA-1**.

   The default setting, SHA-1, is the most common and interoperable hash algorithm that is used by applications and operating systems. For more information about CSP support on computers that are running Windows 2000, see "Microsoft Enhanced CSP Is Not Supported for Certificate Services Installations" on the Microsoft Knowledge Base.

7. In **Key length**, select **2048**.

   There is no verification of the key length that you type into the box. Because of this, verify that the key length is interoperable with organizational applications and other PKI components.

8. Verify that both the **Allow this CSP to interact with the desktop** and **Use an existing key** check boxes are cleared, and then click **Next**.
9. In **Common name for this CA**, type a common name for the CA. For this example, type **IntermediateCA1**.

   As it is specified in the CPS, you must specify the common name (CN) for this CA. The CN cannot exceed 64 characters in length; however, it is recommended that you use a maximum CN length of 51 characters to prevent encoding length rule violation.
10. (Optional) In **Distinguished name suffix**, type the distinguished name suffix for the CA, and then click **Next**.

    If you type a distinguished name suffix in **Distinguished name suffix**, confirm that you have typed the name correctly so that it works in the context of the Active Directory domain name. In the Contoso scenario, the distinguished name is ***DC=concorp,DC=contoso,DC=com***.
11. The CA certificate's validity period for a subordinate CA is always determined by the parent CA. For more information, see "Set the validity period for issued certificates at the offline root CA," earlier in this document.
12. If you have uninstalled a CA on this computer already, you receive a warning message that confirms that you want to overwrite the private key from the previous CA installation. It is recommended that you ensure that the private key is never required again. If you make a backup copy of the system, it is more likely that you will not lose any data. (You can also make a backup copy of the private key as an alternative to a system backup. To do this, at a command prompt, type **certutil –backupkey -?**) If you are not sure if you want to overwrite the private key, click **No** to cancel the installation procedure. If you click **Yes**, a new key is generated and the new key replaces the existing key.

    The key pair is generated by the CSP and written to the local computer's key store.
13. On **Certificate Database Settings**, confirm that **Certificate database**, **Certificate database log**, and **Shared folder** are set to the folder that you want to use.
14. (Optional) To install a CA in the same location as a CA that was installed previously, select the **Preserve existing certificate database** check box, and then click **Next**.
15. In **Shared folder**, confirm that the specified folder is set to a local path, such as C:\CAconfig, and then click **Next**.
16. Insert the Transfer-IntermediateCA floppy disk into the disk drive.
17. On **CA Certificate Request**, click **Save the request to a file** and, in **Request file**, type a name for the request file that will be saved to the floppy disk, and then click **Next**.

    The file must have a .req extension, such as a:\IntermediateCA1.req.
18. If you receive a message that IIS must be stopped to continue the installation, click **Yes**.

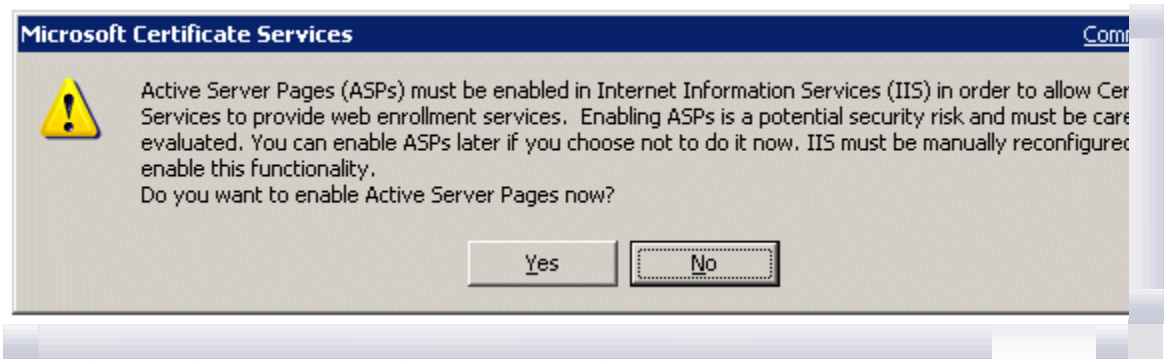
    The intermediate CA needs to submit the certificate request to its parent offline CA. Because the CorporateRootCA computer is running without a network connection, you must transfer the requested file on a floppy disk.

    Caution Verify that the floppy disk is available before you proceed. If the storage device is not accessible, you receive an error message, the CA setup procedure stops, and you must reinstall the CA. Before you can reinstall the CA, you must uninstall Certificate Services Web-Enrollment Support if it was supposed to be installed.
19. The Windows Component Wizard completes the certificate services configuration.

    When the CA certificate has obtained a signed subordinate CA certificate from its parent CA, the wizard displays a message which says that the installation has finished. Make sure that the local storage device is available to save the request file, and then click **OK**.
20. Click **Yes** to enable ASP pages that are required for Web enrollment services.

    IIS is installed for illustration purposes as part of this configuration, but Active Server Pages (ASP) pages are not enabled by default. Because of this, the CA setup procedure provides an option to automatically enable the ASP pages.

    If you click **No**, you can enable ASP by typing **certutil –vroot** at a command prompt at a later time.



If your browser does not support inline frames, click here to view on a separate page.

Figure 8 Enable Active Server Pages

21. After the wizard finishes installing files, click **Finish,** and then click **Close**.
22. Remove the **Transfer-IntermediateCA** floppy disk from the disk drive, and then take the floppy disk to the parent CA (CorporateRootCA).

Verify the Certificate Request

Before the certificate request is submitted to the parent CA, verify that the policy identifier that you set in the CA configuration through CAPolicy.inf is correct. If the syntax of the CAPolicy.inf file is incorrect, certain configuration information may be missing from the request file. To verify that all configuration information is properly included in the certificate request, view and examine the request file. To verify the request file, at a command prompt, type **certutil** *RequestFile*, where *RequestFile* is the request file that you save to the floppy disk, including the correct path, and then press ENTER.

The command produces output that is similar to the following output. Verify that the Certificate Policies section is correct as well as all of the other information that is specified in the CAPolicy.inf file.

If the Certificate Policies section does not appear in your certificate request, see "Prepare the CAPolicy.inf file for IntermediateCA1," in this document, correct the syntax in the CAPolicy.inf file, and then repeat the subordinate CA installation procedure.

```
  Attribute[2]: 1.2.840.113549.1.9.14 (Certificate Extensions)
    Value[2][0]:
    Unknown Attribute type
Certificate Extensions: 6
    1.3.6.1.4.1.311.21.1: Flags = 0, Length = 3
    CA Version
        V0.0

    2.5.29.14: Flags = 0, Length = 16
    Subject Key Identifier
        84 b9 bf 37 a7 9b 0d 75 28 62 00 27 bf 72 da d0 66 a5 79 e8

    2.5.29.32: Flags = 0, Length = 139
    Certificate Policies
        [1]Certificate Policy:
             Policy Identifier=1.3.6.1.4.1.311.21.43
             [1,1]Policy Qualifier Info:
                  Policy Qualifier Id=User Notice
                  Qualifier:
                       Notice Text=Legal policy statement text.
        [2]Certificate Policy:
             Policy Identifier=1.3.6.1.4.1.311.21.47
             [2,1]Policy Qualifier Info:
                  Policy Qualifier Id=CPS
                  Qualifier:
                       http://www.contoso.com/pki/LimitedUsePolicy.htm
             [2,2]Policy Qualifier Info:
                  Policy Qualifier Id=CPS
                  Qualifier:
                       ftp://ftp.contoso.com/pki/LimitedUsePolicy.txt
             [2,3]Policy Qualifier Info:
                  Policy Qualifier Id=User Notice
                  Qualifier:
                       Notice Text=Limited use policy statement text.
```

Certificate Request Processing with the Root CA through MMC

The subordinate CA certificate request that is saved on the **Transfer-IntermediateCA** floppy disk must be signed by the parent (CorporateRootCA).

You can submit a request to an offline CA by using either the Certification Authority MMC or the Web Enrollment page that is on the parent Windows Server 2003 CA. You can also submit the request by typing **certreq.exe –submit** at a command prompt. All methods allow you to submit a certificate request that you have saved to a request file (*.req). This section will present the first method, using the Certification Authority MMC. For more information on using the Web Enrollment page, see "Certificate request processing with the offline parent CA (IntermediateCA1) through Web-Enrollment Support," later in this document.

Caution If a previous CA setup procedure did not work and you repeat the setup procedure, do not reuse the request file from the earlier CA setup procedure. It has an association with previous key material that will not be associated with the current CA that you are installing.

If a CA is set up, the key material is generated and the certificate request is submitted to the parent CA. The relationship between key material and certificate is maintained by the **AKI certificate** attribute. To ensure that the association of the CA key pair and certificate request matches, a unique request file must be used when a CA is set up.

1. Log on to the CorporateRootCA computer as a CA administrator.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Certification Authority**.

   You can also click **Start**, click **Run**, type **certsrv.msc**, and then press ENTER.
3. In the console tree, right-click the certification authority you are working with, point to **All Tasks**, and then click **Submit new request**.
4. Insert the Transfer-IntermediateCA floppy disk into the CorporateRootCA computer's floppy disk drive, browse to the disk drive, click the certificate request file, and then click **Open**.
5. A stand-alone CA typically issues certificates only after a manual issuing process. (You can change the request handling on the Policy Module tab of the CA's Properties.) In the default configuration, you must manually issue the certificate request by the parent CA:
   a. In the Certification Authority MMC console tree, under the name of the CA you are working with, double-click the **Pending Requests** container.
   b. In the details pane, right-click the appropriate pending certificate request that corresponds to the submitted subordinate CA request, point to **All tasks**, point to **View Attributes**, and then click **Extensions**.
   c. Click **Certificate Policies**, and then verify that the information is correct.

      If the certificate policy information that is defined in the Intermediate CA's CAPolicy.inf file does not appear here, deny the request and return to "Prepare the CAPolicy.inf file for IntermediateCA1," earlier in this document.
   d. In the console tree, click **Pending Requests**, and, in the details pane, right-click the pending request, point to **All Tasks**, and then click **Issue**.

      The request is processed and the certificate request is removed from the list.

      By default, a stand-alone Windows 2000 or Windows Server 2003 CA issues certificates with only a two-year lifetime. Because the registry key that has an impact on the validity time of the certificate was previously set, the certificate enrollment continues with the value that you specified. For more information, see "Set the validity period for issued certificates at the offline root CA" in this document.
   e. In the console tree, click expand the **Issued Certificates** container and, in the details pane, right-click the certificate, and then click **Open** to verify the certificate as described in the next step..

Verify the IntermediateCA1 Certificate

To ensure that the certificate that was issued for IntermediateCA1 has the correct certificate properties, verify the issued certificate:

1. Because a CA policy is specified for IntermediateCA1, the issued certificate will allow all issuer and all application policies. On the **General** tab, click **Issuer Statement** and verify that the certificate is valid for the following purposes:
   - All issuance policies
   - All application policies.
2. Click **Close** to return to the certificate viewer.

3. Click the **Details** tab, and then verify that the **CRL Distribution Points** and **Authority Information Access** values are the same as the distribution points that are specified . Verify other certificate attributes, as required. If values do not match, see "Configure CorporateRootCA distribution points for CRL and AIA," earlier in this document, to help you correct the configuration.

Note You can also verify the certificate after it has been exported to a file. To view the certificate information from a PKCS #7, .der, or Base64-encoded certificate file, at a command prompt, type the *CertFile* name and hit ENTER. Replace ,*CertFile* with the location and file name of the certificate file.

Export the Offline Intermediate Certificate at the Root CA

If the certificate that was issued for the intermediate CA passes the verification steps, export the certificate from the root CA.

Note Because the Certificate Export Wizard can include the complete certificate path with the exported file, you should use this method instead of the binary export method which only exports a single certificate.

1. Open the Certification Authority MMC.
2. In the console tree, under the CA that you want to work with, click **Issued Certificates**.
3. In the details pane, double-click the subordinate CA certificate you want to work with, click the **Details** tab, click **Copy to file**, and then click **Next**.
4. Click Cryptographic Message Syntax Standard – PKCS#7 Certificates (.P7B), select the Include all certificates in the certification path if possible check box, and then click Next.
5. Type a file name without an extension for the export file, and then save the file on the **Transfer-IntermediateCA** floppy disk.

   For example, you could type **A:\IntermediateCA1**. The file is automatically saved on the floppy disk with a .p7b file name extension.
6. Click **Next**, click **Finish**, click **OK**, and then click **OK** again.

   The certificate contains only public information, because the key material that is associated with the certificate was generated and is stored on the IntermediateCA1 computer. There is generally no need to protect the certificate information that is stored on the floppy disk. The CA certificate and the parent CA certificates are always considered to be public information.
7. In the console tree, click **Issued Certificates**.
8. Right-click the issued certificate in the details pane, point to **All Tasks**, and then click **Export Binary Data**.

   In **Columns that contain binary data**, **Binary Certificate** is the default choice.
9. Click **Save binary data to a file**, and then click **OK**.
10. Insert the **Transfer-IntermediateCA** floppy disk into the drive, in **File name**, enter a file name with a .cer extension, and then click **Save**.

    For example, you could type **A:\IntermediateCA1.cer**. The certificate is then saved in the DER-encoded file format.
11. On the **File** menu, click **Exit**, and then log off of the CorporateRootCA computer.

Install the Certificate on IntermediateCA1

You have now processed the request that was sent to the root CA and saved it on the **Transfer-IntermediateCA** floppy disk. You must now install the signed subordinate CA certificate that belongs to IntermediateCA1. You can install the CA certificate either by running a command at a command prompt or by using the Certification Authority MMC. The subordinate CA certificate request will only be accepted by the parent CA if it carries the requesting CA's signature on the request.

Verify the IntermediateCA1 Certificate Trust Chain

To prevent unexplained or unintentional behaviors, verify the certificate trust chain. You must complete the trust chain verification procedure from a command prompt because the trust path that is displayed in the Certification Authority MMC Snap-in uses a different implementation for chain-building.

1. Log on to the IntermediateCA1 computer as a local administrator
2. At a command prompt, type

   certutil –verify *a:\CACertFile***.crt**

   where a:*CACertFile* is the path and name of the file.

3. Press ENTER to view the full certificate verification results.

This command may generate a lot of output. When **dwErrorStatus** is not equal to zero, a certificate verification error has occurred, so you should verify that **dwErrorStatus** is equal to zero (0) on each line that is produced.

You can also use the following command

certutil –verify *a*:*CACertFile***.crt | findstr /c:"dwErrorStatus"**

where a:*CACertFile* is the path and name of the file.

Output that has completed the CA certificate verification without errors looks like the following sample output:

```
CertContext[0][0]: dwInfoStatus=102 dwErrorStatus=0
CertContext[0][1]: dwInfoStatus=10c dwErrorStatus=0
```

The certificate verification process retrieves any CRL that is necessary to verify the certificates. After the verification process, cached copies of the CRLs are available in the temporary Internet Explorer folder on the client.

Install the Certificate on IntermediateCA1

After you have verified that the certificate trust chain can be properly built, install the CA certificate.

1. Log on to the IntermediateCA1 computer as either a CA administrator or local administrator.
2. Click **Start**, point to **Administrative Tools**, and then click **Certification Authority** to start the Certification Authority MMC Snap-in.
3. In the console tree, right-click **IntermediateCA1**, point to **All Tasks**, and then click **Install CA Certificate**.
4. Insert the **Transfer-IntermediateCA** floppy disk into the floppy disk drive.
5. Browse to the floppy drive, click **IntermediateCA1.p7b**, and then click **Open**.
6. (Optional) If the parent CA certificate has not been previously trusted, you may receive a message that says that the root certificate is not trusted. Click **OK**, and then install the root CA certificate to the trusted root CA certificate store on the local computer.

   The root CA of the certificate chain must be locally trusted so that the CA service can start. For more information, see "Import the root CA certificate and CRL to the intermediate CA," earlier in this document.
7. In the console tree, right-click the name of the stand-alone offline intermediate CA, point to **All Tasks**, and then click **Start Service**.

   This brings the stand-alone offline intermediate CA into an operational state by starting the CA service. You can also type **net start certsvc** at a command prompt.

   Note that, after the CA has been started successfully, the icon that displays the CA's operational state turns into a green check mark.
8. On the **File** menu, click **Exit** to close the Certification Authority MMC.
9. Log off of the IntermediateCA1 computer.

Continue the installation procedure by following the steps in the Installation cleanup section in this document.

Install the Certificate at IntermediateCA1

To install the certificate at a command prompt:

1. Log on to the computer as a local administrator with CA Management permissions.
2. At a command prompt, type

   certutil.exe –installcert A:\IntermediateCA1.p7b

   Note If you used a .cer file instead of a p7b file and you receive a warning message at the end of the output such as "A certificate chain was processed, but terminated in a root certificate which is not trusted by the trust provider. 0x800b0109 (-2146762487)," it is possible that the parent CA certificate has not been imported into the local computer certificate store or that the parent CA certificate has been saved to the wrong store. To correct this error, see "Import the root CA certificate and CRL into an intermediate CA from a batch file," later in this document. To resolve this behavior, you can also use a PKCS#7 file (a .p7b file) that includes the entire certificate chain instead of a binary certificate file.
3. To start the CA service, at a command prompt, type **net start certsvc**.

Installation Cleanup

For security reasons, it is recommended that you delete the certificate request file on the **Transfer-IntermediateCA** floppy disk that you used to generate the CA certificate.

Configure IntermediateCA1

After you complete the steps in the previous sections to configure the offline CA, you can complete the remaining steps for IntermediateCA1 with a batch file script. The difference between the root CA configuration and the subordinate CA configuration is the validity period for issued certificates. To configure the subordinate CA:

1. Log on to the IntermediateCA1 computer as local or CA administrator.
2. Start a text editor, such as Notepad.
3. In this document, copy the sample text in "Sample script to configure IntermediateCASample" to a new document in the text editor.
4. Save the text file as **%temp%\subcacfg.cmd**.
5. Close the text editor.
6. At a command prompt, type **%temp%\subcacfg.cmd**, and then press ENTER.

Include CA Policy in Certificate Requests

The option around the CA issuer and application policies is a choice at which CA level the policy is applied. If you plan to configure a issuer statement at a CA, you must configure the parent CA to add information about the CA policy to its issued certificates. See "Sample CAPolicy.inf file for the IntermediateCA1" later in this paper.

If this configuration step is skipped, an intermediate CA will not accept or allow CA certificate policies from its subordinate CAs. If required, you can apply this configuration step at the time when a issuer or application policy needs to be included in a certificate request from a subordinate CA.

To include a policy in issued certificates, enter the following commands at a command prompt:

```
certutil -v -setreg policy\EnableRequestExtensionlist "+2.5.29.32"
certutil –shudown
net start certsvc
```

You can disable the setting with **certutil -v -setreg policy\EnableRequestExtensionlist "-2.5.29.32"**

```
certutil –shudown
net start certsvc
```

Verify the IntermediateCA1 Configuration

After you use the steps in the previous sections, ensure that the CA is configured properly and ready for production operations. You should apply the verification steps as described in the following sections in this document because they apply to the intermediate CA the same way as for a root CA:

- Verify the root CA configuration
- Verify the CorporateRootCA CRL and AIA configuration
- Verify the published CRL

Finalize the CA Configuration

After you apply the steps from the previous sections in this document, the intermediate CA is operational and ready to issue certificates.

If you installed a Windows 2000 CA instead of a Windows Server 2003 CA, you should apply the additional configuration steps that are explained in the "Disable issuer name and issuer serial number" section in this document.

Stand-alone Offline Intermediate CA (CorporateSub2CA)

The sample PKI topology design has exemplified two separate offline intermediate stand-alone CAs that provide organizational and security flexibility. The CorporateSub2CA setup is similar to the steps that are outlined for IntermediateCA1. The only differences will be some of the configuration parameters, depending on the guidelines that are specified in the organizational CPS.

To apply the sample design, install IntermediateCA2 using the identical steps for installing IntermediateCA1.

Online Enterprise Issuing CAs (CorporateEnt1CA)

The online enterprise issuing CA is also referred to as "CorporateEnt1CA" in this document. The purpose of an

enterprise CA is to automate certificate enrollment without making compromises in the security and authentication of issued certificates.

Depending on the PKI topology that you implement, this CA might have at least one parent CA or, in a single tier topology, it might be a self-signed CA.

When you set up either a Windows Server 2003 Server enterprise CA or Windows 2000 Server enterprise CA, it is important to note that domain controllers in an Active Directory environment automatically request certificates when an enterprise CA) becomes available in the forest.

The automatic certificate request behavior is different between computers that are running Windows 2000 or Windows Server 2003 domain controllers. Windows 2000 domain controllers immediately start requesting certificates when the enrollment service is available; however, a Windows Server 2003 domain controller requests certificates according to the Autoenrollment configuration in Group Policy settings. Computers that are running Windows Server 2003 domain controllers and computers that are running Windows XP request certificates, according to the configuration of the Group Policy object (GPO). You must enable the request processing manually, by using the appropriate domain Group Policy. Note that domain controllers have their own GPO settings which are separate from the rest of the computers in the domain. To add an automatic request setting for Windows 2000 domain controllers, create a new request object in the following GPO path using the following procedure.

1. Click **Start**, click **Run**, type **mmc**, and then press ENTER
2. In the console tree, double-click the domain controller policy that you want to work with, double-click **Computer Configuration**, double-click **Windows Se**ttings, double-click **Security Settings**, double-click **Public Key Policies**, and then click **Automatic Certificate Request Settings**.
3. In the details pane, right-click a blank area, point to **New**, and then click **Automatic Certificate Request**.
4. Follow the instructions in the Automatic Certificate Request Setup Wizard.

For more information on configuring auto-enrollment for Windows Server 2003 domain controllers, see "Certificate Autoenrollment in Windows XP" on the Microsoft Web site.

Enterprise CA Installation Prerequisites

The following items are required to correctly install and configure the online enterprise CA:

- The CPS that has all of the parameters that are specific to your organization. For more information, see "Certificate practice statement," earlier in this paper.
- The Windows Server 2003, Enterprise Edition media
- Appropriate hardware and a floppy disk drive
- A floppy disk that is labelled **Transfer-EnterpriseCA**
- The computer must be joined to a domain in the appropriate Active Directory forest
- Local administrator, Enterprise Administrator and Root Domain Administrator permissions
- File and print sharing is enabled on the CA. This is required to run the certification authority MMC snap-in on the CA.
- If you are using a Windows 2000 Active Directory forest, the domain controllers must have Service Pack 3 (SP3) applied for computers that are running Windows 2000. It is also required to upgrade the schema to Windows Server 2003 functionality as previously described. For more information, see "HOW TO: Raise the Domain Functional Level in Windows Server 2003" on the Microsoft Web site.

To correctly install and configure the online enterprise CA using Windows 2000 Server, the following articles may provide useful information:

- For a Windows 2000 CA configuration, see "Step-by-Step Guide to Setting up a Certification Authority" on the Microsoft TechNet Web site:
- For more information about how to submit a certificate request through Windows 2000 Certificate Services Web enrollment support, see "Step-by-Step Guide to Setting Up a Certificate Authority" on the Microsoft TechNet Web site.

You should also ensure that the following tasks have been completed:

- A server running Windows Server 2003, Enterprise Edition should be set up and available to be used as the enterprise CA.
- The server should have the latest service packs available and installed, if appropriate.
- The server that is hosting the CA service must be joined to a domain in the Active Directory forest.

It is possible to install a CA as a multiservice server or as a domain controller, but this is not recommended for security reasons. A CA has high security requirements and should be accessed and maintained only as separate

resource.

Prepare the Active Directory Environment

You can operate an Windows Server 2003 enterprise CA in a Windows 2000 environment if all domain controllers in the Active Directory are running Windows 2000 SP3 or later. Windows 2000 SP3 domain controllers are the minimum version required to support the schema upgrade for version 2 templates, as described in the previous chapter..

The schema upgrade, which does not cause a full replication in a Windows Server 2003 domain environment, is required to add additional template information, key archival information, cross-certificate objects, and object identifier (also known as OID) objects in the directory.

It is assumed that the schema upgrade is part of the organization change and management process as it can have an overall effect on the production environment.

To upgrade the schema:

1. Log on to the schema master domain controller as the Schema Administrator.

   For more information regarding schema administrator roles, see "HOW TO: Find Servers That Hold Flexible Single Master Operations Roles" in the Microsoft Knowledge Base.

2. Make the Windows Server 2003, Enterprise Edition, installation media available to the server and, at a command prompt, type the following command, and then press ENTER.

   adprep /forestprep

   The Adprep.exe file is available from the \i386 directory on the original Windows Server 2003, Enterprise Edition, installation media: After you use this command, you receive an output that contains logging information about the schema-upgrade process. The output ends with the message "Adprep successfully updated the forest-wide information."

To enable the domain to benefit from the Windows Server 2003 schema extensions, you must perform the following procedure on each domain in the forest.

1. Log on to the domain as Domain Administrator.
2. At a command prompt, type:

   adprep /domainprep

3. Repeat the previous two steps for each domain in the forest.

Depending on the replication schedule, the time required to apply the schema changes at each domain controller in the forest will vary.

Domain Membership

An enterprise CA can enroll any user or machine in the forest. To enable the CA to issue certificates to users and computers that are members of other domains than the domain where the CA is installed, see the Windows Server 2003 Server Help files or the following articles in the Microsoft Knowledge Base:

- Windows 2000 Certification Authority Configuration to Publish Certificates in Active Directory of Trusted Domain on the Microsoft Knowledge Base
- Enterprise CA May Not Publish Certificates from Child Domain or Trusted Domain on the Microsoft Knowledge Base

If the organization's Active Directory consists of several domains, you should plan where to put the enterprise CAs. There are three different approaches that you can take. Note that you must evaluate these approaches according to the requirements and the Active Directory design. Enterprise CAs can be:

- Installed into each production domain.
- Maintained in a separate PKI domain.
- Maintained as members of the forest root domain.

When you run enterprise CAs as members of the forest root domain, isolation and logical grouping is ensured but might not be accepted by the forest root administrator group because of security considerations. All approaches are valid, but must be carefully considered for your environment.

Retrieve the Certificate and its CRL from CorporateRootCA and IntermediateCA1

Note If you implement a single-tier topology, the steps in this section do not apply to your environment.

Both the certificate and CRL for all nodes in the PKI hierarchy are required during certificate validation.

Because all parent CAs of an issuing enterprise CA might be disconnected from the network (as in this sample

scenario), you cannot automatically retrieve the CA certificates and the latest CRLs through the network when required. Because of this, you must make the CA certificates and the most current CRL available from all parent CAs before you can set up CorporateEnt1CA.

If the certificate of CorporateRootCA is not available on the **Transfer-RootCA** floppy disk, perform the steps that are outlined in "Obtain the certificate and its CRL from CorporateRootCA," earlier in this document.

You can retrieve the certificate and CRL for illustration purposes from IntermediateCA1 through Web enrollment support on the CA. Internet Information Services is not required to retrieve the CA certificate and CRL from the root CA as they may copied from the %systemroot%\system32\certsrv\certEnroll\ path on the local system. To retrieve the CA certificate and CRL through the web pages, perform the following steps:

1. Log on to the IntermediateCA1 computer.

   If the CA is accessible from the network, you can use any other computer to download the CA certificate and the CRL; however, these tasks require an interactive local logon because the CA is disconnected form the network.
2. Click **Start**, and then click **Internet Explorer**.
3. In **Address**, type **http://localhost/certsrv**.

   Localhost is an alias name for your current server. The Welcome page from IntermediateCA1 Web enrollment support is displayed.
4. Click **Download a CA certificate, certificate chain or CRL**
5. Insert the **Transfer-IntermediateCA** floppy disk into the disk drive.

   Next, download the CA certificate chain.
6. Click **Download CA certificate chain**, and then click **Save**.
7. In **Save As**, type a file name (for example, type a:\IntermediateCA1.p7b), and then click **Save**.

   Next, download the latest base CRL:
8. Click **Download latest base CRL** and then click **Save**.
9. In **Save As**, type a file name (for example, type a:\IntermediateCA1.crl), and then click **Save**.

   If applicable to your environment, download the latest delta CRL:
10. If applicable, click **Download latest delta CRL**, and then click **Save**.
11. In **Save As**, type a file name (for example, type a:\IntermediateCA1+.crl), and then click **Save**.
12. Remove the **Transfer-IntermediateCA** disk from the disk drive.

Distribute a Root CA Certificate with Group Policy

Note If you implement a single-tier topology, the steps in this section do not apply to your environment, because an enterprise CA that is configured as the root CA automatically publishes certificates to Active Directory.

If a single tier topology is implemented, the steps in this section do not apply because an enterprise CA that is configured as the root CA would publish its certificate automatically into Active Directory.

The validation of certificates requires the availability and explicit trust of the root CA certificate that has issued certificates within the certificate trust path. The root CA certificate provides the trust anchor from which PKI hierarchies are derived.

The easiest way to provide clients with the root CA certificate is through group policies. Trust of root certification authorities should be managed and controlled through Group Policy whenever possible. When a root CA certificate has been added to the Trusted Root certification authority’s container that is part of the domain security settings, clients that are member of the domain will receive the root certificate automatically.

Warning You must not publish subordinate (or intermediate) CA certificates through either the trusted root certification authorities in Group Policy or an enterprise trust. If a subordinate CA certificate is part of this list of certificates that is published with Group Policies, a Windows client will not build a certificate chain correctly.

The security portion of a domain Group Policy setting distributes the list of trusted root certificates to all computers that are Active Directory-aware and members of a domain. Because the root certificate becomes part of the computer policy, all domain-users inherit the root certificate trust from the computers to which they logon.

Note

- It is recommended that you make a copy of the default domain policy and use a new policy specific to PKI to administer PKI policy in the domain.

- Modification of any of the default values requires more in-depth planning regarding certificate trusts and name constraints.
- Group Policy displays a slightly different view in a Windows 2000 environment. but it provides the same functionality.

To add the root CA certificate of CorporateRootCA through Group Policy to the list of trusted root CA certificates on all computers in the domain, use the following procedure.

1. Log on as the domain administrator to the domain where you want to deploy the root CA certificate.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Domain Security Policy**

   You can also type **Dompol.msc** at a command prompt and then press ENTER.
3. In the console tree, double-click **Default Domain Policy**, double-click **Computer Configuration**, double-click **Windows Settings**, double-click **Security Settings**, and then click **Public Key Policies**.
4. Right-click Trusted Root Certification Authorities, click Import, and then click Next.
5. Insert the **Transfer-RootCA** floppy disk, and then click **Browse**.
6. Click **Open** to select the certificate file.
7. Click Place all certificates in the following store. After the certificate is placed in the Trusted Root Certification Authorities container, click Next.
8. After a report displays the options that you have selected in the wizard, click **Finish** to import the certificate.

You can configure additional PKI trust properties by using the Trusted Root Certification Authorities Properties page. To set these properties, right-click **Trusted Root Certification Authorities**, and then click **Properties**.

If you disable the default third-party root CAs and enterprise root CAs option, there may be unintended effects when you try to gain access to applications such as SSL secured Web sites on the Internet, and so on.

When only enterprise root certificates are trusted, only CA certificates that are installed in the following container in the configuration partition of Active Directory or through Group Policy are trusted: Domain Name\Configuration\Services\Public Key Services\Certification Authorities.

See the Sites and Services MMC to verify the certificates. You must make the services node visible to see the Services container.

Import Parent CA Certificates and CRLs into Active Directory

The following section outlines the procedures for publishing the CA certificates and CRLs of offline CAs (CorporateRootCA, IntermediateCA1, and CorporateSub2CA) into Active Directory.

> **Important** Do not use the information in this section if you are implementing a single-tier CA because a single tier enterprise root CA publishes it's root Certificate automatically into Active Directory.

You must import offline CA certificates and their CRLs. Note that this import procedure for the publication of CA certificates must be repeated every time that the offline CA's certificate is renewed.

Also the CRL must be imported according to the CRL publication strategy. Every time that a new CRL is published by the parent CA, you must repeat the publication procedure. To prepare the environment for the enterprise CA installation, you must register the parent CA certificates and CRLs in Active Directory. For information about how to do this, see the following section in this document.

Get CA Sanitized Name and DNS Name

The configuration information that is part of the CRL in Windows Server 2003 is different from the configuration information that was included with versions of the Windows 2000 family. A CRL that was published by a Windows 2000 CA does not contain information about the publication location of the CRL. (For more information, see "Verify the published CRL" in this document.) However, you must know where you want to save the CRL during the import process into Active Directory.

A Windows Server 2003 CA stores this information in the optional **Published CRL Locations** attribute of a CRL if the corresponding CRL property was set. When you perform a CRL import procedure on a computer that is running a Windows 2000 operating system, you must manually set the path of the CRL publication location.

To display the CA's computer name and the CAs sanitized name, at a command prompt, type the following and then press ENTER.

certutil –cainfo

You can also use this command on a Windows 2000 CA that should be published to Active Directory. It is important that you note both the sanitized CA short name (DS name) and DNS name for each Windows 2000 CA. A sample output from the command is similar to the following output, where the items in bold are

placeholders:

```
Exit module count: 1
CA name: IntermediateCA1
Sanitized CA short name (DS name): IntermediateCA1
CA type: 4 -- Stand-alone Subordinate CA
    ENUM_STANDALONE_SUBCA -- 4
CA cert count: 1
KRA cert count: 0
KRA cert used count: 0
CA cert[0]: 3 -- Valid
CA cert version[0]: 0 -- V0.0
CA cert verify status[0]: 0
CRL[0]: 3 -- Valid
CRL Publish Status[0]: 5
    CPF_BASE -- 1
    CPF_COMPLETE -- 4
Delta CRL Publish Status[0]: 0xe (14)
    CPF_DELTA -- 2
    CPF_COMPLETE -- 4
    CPF_SHADOW -- 8
DNS Name: connoam-ca-00
Advanced Server: 1
CertUtil: -CAInfo command completed successfully.
```

If either the CRL path that is specified in the CRL or the path where the CRL is physically published is not the same, an issuer distribution point (IDP) intersection error might appear when the CRL is verified by a client.

Import CA Certificates and CRLs from CorporateRootCA and CoporateSubxCA

In order to continue the installation procedure, you must import CA certificates and CRLs from parent offline CAs into Active Directory. In general, this procedure is a common operation when the CA environment is set up. CRL publication and distribution with Active Directory is critical for a successful PKI in your organization. Importing root CA certificates into the Active Directory directly is preferred over using Group Policy to distribute root CA certificates, as this method provides for root CA trust throughout the entire forest instead of individual domains.

Both, the CA certificate and CRL are written by the **Certutil.exe** utility into Active Directory. Note that **Certutil.exe** replaces the **Dsstore.exe** utility that is available in the Windows 2000 Resource Kit. For more information, see "HOW TO: Use the Directory Services Store Tool to Add a Non-Windows 2000 Certification Authority (CA) to the PKI in Windows 2000" on the Microsoft Knowledge Base and "The Dsstore Tool May Not Work If the NetBIOS Name and the DNS Domain Name Are Different" on the Microsoft Knowledge Base.

> **Caution:** Do not use the **Dsstore.exe** utility that is included with the Windows 2000 Resource Kit to import CA certificates and CRLs to a Windows Server 2003 environment.

To import CA certificates and CRLs from parent offline CAs into Active Directory, use the following procedure:

1. Log on to the CorporateEnt1CA computer as **Administrator** of the **Root-Domain** and also a member of the **Enterprise Administrators** group.
2. At a command prompt, use the following sample script to import CA certificates and CRLs from CorporateRootCA and CoporateSubxCA to Active Directory. Note that you must change the script so that both the CA certificates and CRLs correspond to your file names and CA names:

```
:
: Root CA certificates
:
certutil -dspublish -f concorp-ca-00_CorporateRootCA.crt RootCA
:
: Sub CA certificate
:
certutil -dspublish -f connoam-ca-00_IntermediateCA1.crt SubCA
:
: Root CA CRLs
: Since these are .NET CA CRLS that have the publication location as
: part of the CRL, the publication location is optional
:
:                                              |-- publication
location ---|
:
certutil -dspublish -f CorporateRootCA.crl     concorp-ca-00
CorporateRootCA
:
: Sub CA CRLs
```

```
:
certutil -dspublish -f IntermediateCA1.crl     connoam-ca-00
IntermediateCA1
```

Note The **–f** parameter is required because the container structure that is required to store the certificates and CRLs and might not exist. The **–f** parameter is not required if the container structure already exists.

Deploying the root CA certificate with Group Policy or Active Directory is not the only way that you can provide clients with certificates of trusted root CA certificates. You can also deploy root CA certificates by using the following methods:

- The Internet Explorer Administration Kit (IEAK)
- A CAPICOM script (For more information, see "CAPICOM Reference" on the Microsoft TechNet Web site.)

Set the Appropriate Permissions for Certificate and CRL access

The CA administrator must ensure that any client in the PKI can gain access to both the CRL distribution points and CA certificate.

For HTTP URLs, it is recommended that Internet Information Services (IIS) be set up and configured to allow anonymous access to the URLs that are set as CRL distribution points in issued certificates. When you do this, clients, regardless of their primary authentication mechanism, can retrieve the CRL.

For URLs that point to a CRL object in Active Directory, the Everyone group has read access by default. To allow clients that are not Active Directory members to gain access to CRL objects in Active Directory, you must add the Everyone group with read permissions to the domain object's ACL. A more restrictive method that you can use to configure anonymous access is to replace the Everyone built-in account with the Anonymous built-in account.

For more information about how to add Read access permissions to clients that are outside of the forest, see the following Microsoft Web sites:

- "Anonymous Queries" in the Windows 2000 Resource Kit
- "How to Use the RestrictAnonymous Registry Value in Windows 2000" in the Microsoft Knowledge Base

Publish CA Certificates and CRLs of CorporateRootCA and CoporateSub1CA

Publishing the CRLs using HTTP requires a Web server, such as IIS. To set up IIS to provide the CRL publishing point using HTTP, use the following procedure:

1. Log on as a local administrator to the computer that has IIS installed.
2. Click **Start**, click **All Programs**, point to **Administrative Tools**, and then click **Internet Information Services (IIS)**.
3. Double-click the IIS server node, and then double-click **Web Sites**.

   The organizational Web site that will host the CRL is displayed.
4. Right-click your Web site, point to **New**, click **Virtual Directory**, and then click **Next**.

   The Virtual Directory Creation Wizard starts.
5. Type an alias name for your Web site (for example, type **PKI**), and then click **Next**.
6. Choose a path where the certificates and CRL will be stored on the a local storage device, and then click **Next**.

   In this example, the CA certificates and CRLs are stored in **C:\PKI**.
7. Select the **Read** check box, clear all of the other check boxes, and then click **Finish**.

   No other permissions are required.
8. Copy the CA certificate and CRLs from the **Transfer-RootCA** floppy disk into the C:\PKI folder. Repeat this step with the CA certificate and CRLs stored on the **Transfer-IntermediateCA** floppy disk.

Note Make sure that the file names that are published with HTTP exactly match the CA certificate and CRL distribution point as defined as part of the CA configuration. If the file names do not match, clients will fail to retrieve the CRL with the URL that was specified as the CRL distribution point.

Verify that the Domain Controller Has Published the Certificates and CRL into Active Directory

After you import the list of CA certificates and CRLs into Active Directory, verify that the data is published to the correct location.

Note In a distributed environment, a delay occurs before any domain controller has received the

certificates and CRLs through Active Directory replication. The delay will vary depending on the Active Directory environment configuration.

You can verify that the CA certificates and CRLs are published to the correct location through the Active Directory Sites and Services MMC Snap-in.

1. Log on to the CorporateEntxCA computer as the administrator of the root domain and as a member of the Enterprise Administrators group.
2. Open the Active Directory Sites and Services MMC, by doing one of the following
   - To use the Windows interface, click **Start**, click **All Programs**, point to **Administrative Tools**, and then click **Active Directory Sites and Services**.
   - To use a command prompt, at a command prompt, type **dssite.msc**.
3. Click **Active Directory Sites and Services**.
4. On the **View** menu, click **Show Services Node**.
5. Click **Services**, and then click **Public Key Services**.
6. Verify that the AIA container has all parent CA certificates, and then verify that the CRL container has the CRL objects for each CA.

   The AIA container has a flat object structure but the CRL distribution point container stores CRLs in a separate container for each CA.

If the AIA or CRL container do not have the proper objects, it may be necessary to manually republish the objects as described above.

To delete certificates or CRLs that are expired, revoked, or no longer required through the Active Directory Sites and Services MMC, click the certificate or CRL and then press DELETE. Keep in mind that clients will need CA certificates to verify end-entity certificates. Even a revoked or expired CA certificate can be required to verify a certificate chain!

Verify That the CA Certificate and CRL Are Imported into Active Directory

To ensure that the correct CRL and AIA information is published to Active Directory, verify the certificate of IntermediateCA1. If clients cannot retrieve a CRL from the CRL's distribution point or do not download a certain CA certificate from Active Directory, the client applications will generate an error when verifying a certificate's status.

Note If the verification procedure in this section does not work, it is important to investigate the cause of the failure. If the publication location in Active Directory is incorrect, correct the location by using the steps in the "Publish CA certificates and CRLs of CorporateRootCA and CoporateSub1CA to a Web site" section in this article.

To verify that the CA certificate and CRL were imported correctly into Active Directory:

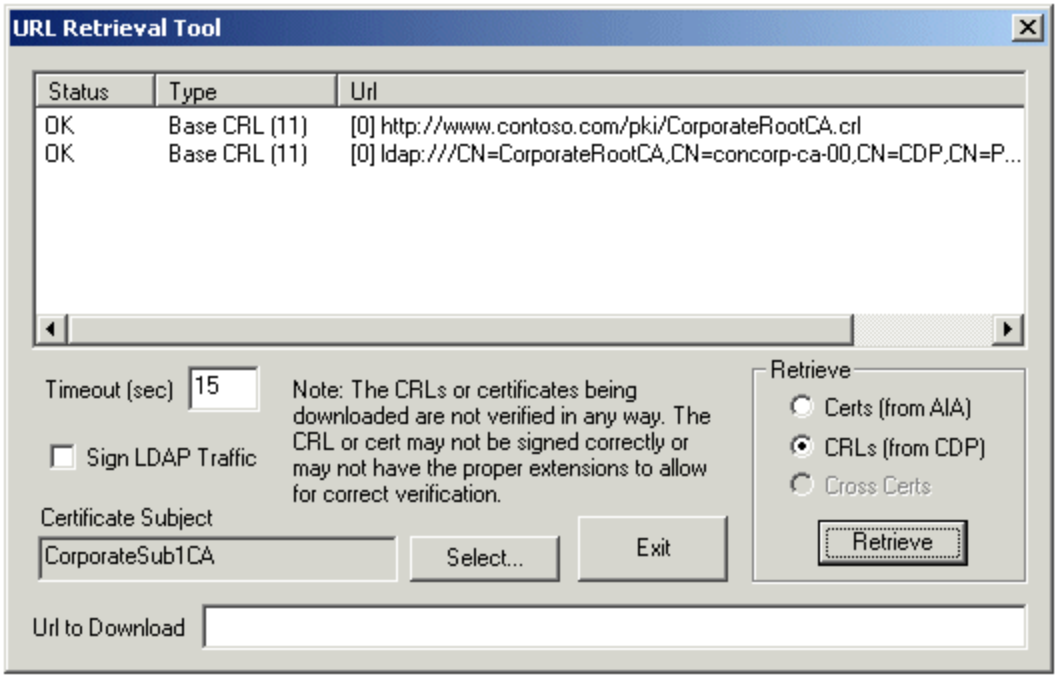
1. Log on to a computer that is member of the organization's Active Directory. The user account that you use can be a domain user account because any user should have read permissions to both the CA certificate and CRL in Active Directory.
2. Insert the **Transfer-IntermediateCA** floppy disk into the floppy drive
3. At a command prompt, type the following, and then click **Retrieve**:

   certutil.exe -url a:\IntermediateCA1.cer

   The **certutil.exe –url** command works with any X.509V3 certificate. You can also use this command to verify user certificates. You can perform CRL and AIA distribution point verification by using the Certutil.exe utility only on certificate files that are Distinguished Encoding Rules (DER) encoded (*.cer file). If you discover that the CRL distribution point is incorrectly configured, you must correct the issue in the CA configuration to which the CRL belongs. The CRL distribution point is stored as an attribute in every issued certificate. Also, there may be an impact on certificates that are already enrolled if the CRL is not correctly configured.

   When you click **Retrieve**, Windows performs a CRL or AIA download based on the certificate file that has been specified. The certificate's name is displayed in **Certificate Subject**.

   Windows lists the certificate's CRL distribution points that are specified in the CRL distribution point extension of the certificate and displays the verification status. The following figure is an example of a successful verification procedure.



If your browser does not support inline frames, click here to view on a separate page.

Figure 8 URL Retrieval Tool

If the CRL verification procedure does not work, the CRL distribution point extensions may not be valid, or the locations of the CRLs have permissions set that do not allow the current user to retrieve the object.

4. In the **Retrieve** box, click **Certs (from AIA)**, and then click **Retrieve**.

   Since the root CA certificate has no CRL defined in this scenario, you receive a CRL status message saying "No CRL." The missing CRL status is expected in this example, since the CRL distribution point was set to Empty in the root CA's CAPolicy.inf file.

Template Upgrade from Windows 2000

When you upgrade from Windows 2000 to a member of the Windows Server 2003 family, you must upgrade both the properties and security settings on existing version 1 (V1) templates.

To perform the upgrade to a Windows Server 2003, Enterprise Edition, CA environment, open the Certificate Templates MMC that is included with Windows Server 2003, Enterprise Edition, so that you can install and upgrade the template objects. It detects that templates are available from a previous Windows 2000 CA installation and automatically upgrades the templates.

The upgrade procedure also changes the permissions that are required for template administration. In Windows 2000, you must be a member of both the Enterprise Admins group and Root Domain Admins group to perform this operation. For more information on certificate templates, see "Implementing and Administering Certificate Templates in Windows Server 2003" on the Microsoft TechNet Web site

Prepare the CAPolicy.inf File for the Issuing CA

If you apply an application or issuance policy at the level where end entity certificates are issued, you have precise control over policies. If more than one issuing CA exists in the PKI hierarchy, different policies can be applied to each CA to issue different certificate types. Nevertheless, policies can be applied at a parent CA level as well. Typically, in most deployments, policies are applied at an intermediate CA level than at the leaf node CA. When you define policies at a parent CA level, the policy applies to all of the subordinate CAs. This could have an impact on the CA topology design.

For an example of a CAPolicy.inf file with issuer policy, see "Sample CAPolicy.inf file for the IntermediateCA1" later in this paper.

Install the Online Issuing Enterprise CA

If you upgrade a Windows 2000 enterprise CA to a Windows Server 2003 CA, you must log on to the computer with an account that is member of both the root domain administrators group and the enterprise

administrators group.

When you perform a clean installation of the first Windows Server 2003, Enterprise Edition CA in a new Windows Server 2003 forest, the installation account requires that you are a member of the Enterprise Admins group and the (root domain) Domain Admins group. After the first CA installation, (root domain) Domain Admins permissions are no longer required.

The installation procedure for an online enterprise CA is different form the installation procedure for the offline parent CAs. Use the following steps to set up CorporateEnt1CA:

1. Log on to the CorporateEnt1CA computer with Local Admin, Enterprise Admin, and (root domain) Domain Admin permissions.

   The installation of an enterprise CA requires that you be able to gain access to the Active Directory configuration container. During the CA installation procedure, the account used to install the CA also becomes a CA administrator account which is a role that can be delegated to other user accounts, as appropriate.

2. Do one of the following:

   - To use the Windows interface, click **Start**, point to **Settings**, click **Control Panel**, double-click **Add or Remove Programs**, and then click **Add/Remove Windows Components**.
   - To use a command prompt, click **Start**, click **Run**, type **cmd**, press ENTER, type **sysocmgr /i:sysoc.inf**, and then press ENTER.

3. Select the **Certificate Services** check box.

   To run Certificate Services, the following software components are required:

   - Certificate Services
   - Internet Explorer
   - (Optional) Certificate Services Web enrollment support
   - (Optional) Internet Information Services for Web enrollment support

   It is not recommended that you install any other Windows components on a Windows Server CA. If you install additional components, reliability or security of a root CA may be compromised if a secure configuration is required by the organization.

4. After you select the **Certificate Services** check box, you receive a warning that states that you cannot change the NetBIOS computer name after you install Certificate Services. (Note also that you cannot change the computer's membership to a domain or workgroup.) Click **Yes** to continue with the installation procedure, and then click **Next**.

   Note IIS is not a required component on an enterprise CA, but it might be necessary to have IIS available for certificate Web enrollment, depending on the enrollment method that is used for clients. Windows 2000 and Windows XP clients typically request certificates by using distributed COM (DCOM) or auto-enrollment instead of HTTP. For more information, see "Authentication and authorization" in this document.

5. When you are prompted to choose the type of installation, do one of the following:

   - If you want this installation to be in a multi-tier PKI topology, click **Enterprise subordinate CA**.
   - If you want this installation to be an enterprise CA in a single-tier topology, click **Enterprise Root CA**. Also, verify that the **Use custom settings** check box is selected.

   In this scenario, the enterprise CA is installed as a subordinate CA. Select **Enterprise subordinate CA**.

   Note that, if the computer that is supposed to be an enterprise CA is a domain member, both the **Enterprise Root CA** and **Enterprise Subordinate CA** options may be unavailable. To find out why the options are unavailable, see the following table.

Table 20 Workarounds for Enterprise Root and Subordinate CA Unavailability

Reason	Workaround
No access to domain controller	The CA cannot gain access to the domain controller through the network. The **nltest.exe /dsgetdc** command might be helpful to iensure connectivity with your domain controller. To use Nltest.exe, install the support tools that are available on the Windows Server 2003 CD-ROM. For more information about nltest see "Active Directory support tools" in the Windows Server 2003 online help or on the Microsoft

	Web site.
Domain controller has not replicated	See "Verify that the domain controller has published the certificates and CRL in Active Directory" earlier in this article.
Configuration container does not exist	See "Verify that the domain controller has published the certificates and CRL in Active Directory" earlier in this article.

After you are done, click **Next**.

6. Do one of the following:
   - If an HSM was not installed, click **Microsoft Strong Cryptographic Provider**.
   - If an HSM was installed, you must click the CSP that was installed during the HSM setup procedure.
7. Select the **SHA-1** hash algorithm.

   SHA-1 is the most common and interoperable hashing algorithm that is used by programs and operating systems.
8. In **Key Length**, select the appropriate setting.

   In this example, set a key length of **2048** for CorporateEnt1CA.
9. Confirm that the **Allow this CSP to interact with the desktop** and the **Use an existing key** check boxes are cleared, and then click **Next**.

   If a CA is already installed on this server, the list of existing keys is created from the system certificates that are stored in the following registry key:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\My\Certificates
10. Set the common name for this CA as specified in the CPS, and then click **Next**.

    Because this CA is an enterprise CA, the distinguished name suffix is predefined to use the namespace of the existing Active Directory's (forest) namespace. It is recommended that this value not be changed.

    The key pair is generated by the CSP and written to the local computer's key store. If an HSM has been installed and selected, the key is generated in the HSM and stored accordingly. If you do not use an HSM, the key is generated by CryptoAPI and stored in the profile of the system account on the local computer. The length of time that is required to generate the key depends on both the size of key that is being generated and the CPU performance of the local computer.
11. Specify the location of the certificate database and the certificate database's log files, and then click **Next**.

    Tip It is a good practice to place both the certificate database and certificate database log on a separate volume from the partition on which Windows is installed for issuing enterprise CAs. This provides increased disk input and output performance and provides sufficient storage space for the database as it becomes larger.

    Because this in an online enterprise CA, the shared folder that stores configuration information is optional. The purpose of the shared folder is to serve clients that do not receive the CA's certificates through the Group Policy object (GPO) or that are not able to retrieve the CA certificates from Active Directory or through Web enrollment support. Any client that has access to the shared folder can import the CA certificates into its certificate store. Depending on the shared folder's name, a new share will be created on the CA server computer. The default name for the shared folder is \\Localhost\CAConfig. If you do not need to publish the CA's certificate and configuration with a shared directory, do not create a shared folder.

    If you are installing a CA in the same location as a previously installed CA, the **Preserve existing certificate database** option is enabled. Click this option if you want the new CA to use this database and preserve the certificates that are in the database; otherwise, the database will be deleted. Use this option only when you want to restore a CA from backup or for CA migration.
12. Click **Save the request to a file**, type a name for the request file, click **Next**, and then click **OK**.

    For example, you can type **a:\CorporateEnt1CA.req**.

    A subordinate enterprise CA needs to send the certificate request to its parent offline CA. Because the IntermediateCA1 computer is running without a network connection, the request file must be transferred on a floppy disk.

    Important Make sure that the **Transfer-CorporateEnt1** floppy disk is available before you proceed to the next step. If Windows cannot access the floppy disk, you receive an error message appears and the CA setup process stops. Before you can reinstall the CA, you must uninstall the **Certificate Services Web-Enrollment Support** component if you selected it during setup.

The Windows Component Wizard continues the certificate services configuration.

When the Windows Component Wizard completes the certificate services configuration, you may need to provide the installation media to finish the installation procedure.

13. When the CA certificate has obtained a signed subordinate CA certificate from its parent CA, the installation wizard displays a final message that indicates that the installation procedure is finished. Before you click **OK**, verify that the **Transfer-CorporateEnt1** floppy disk is available to save the request file.

    Click **OK** to continue the installation.

14. (Optional) If IIS is installed as part of this configuration but ASP pages are not enabled by default, the CA setup procedure asks whether you want to automatically enable the ASP pages. Click **Yes** to enable ASP pages, because they are required for Web enrollment services.

    If you click **No** because you do not want to enable ASP pages, you can enable ASP pages by using the **certutil –vroot** command at a later time

15. Click **Finish** to complete the installation procedure, and then click **Close** to close **Add or Remove Programs**.

16. Remove the **Transfer-**CorporateEnt1 floppy disk from the floppy disk drive, and then take the floppy disk to the parent CA computer (IntermediateCA1).

    If this installation procedure is for an enterprise root CA, continue to "Configure the enterprise online CA" in this document.

Certificate Request Processing with the Offline Parent CA (IntermediateCA1) Through Web Enrollment Support

The following procedures are provided as an example and not necessarily as a security best practice. This information is also available in "HOW TO: Get a Certificate Signed by Off-Network Root Authority" on the Microsoft Knowledge Base.

You do not need IIS on a CA unless you need client support for enrollment on Windows clients earlier than Windows 2000 or non-Windows clients.

In a three-tier topology, the enterprise CA certificate request that is stored on the floppy disk must be issued by the IntermediateCA1 computer. In a two-tier topology, the certificate request must be issued by the root CA.

To Request a CA Certificate Through Web Enrollment Support

1. Log on to the CA computer that will issue the enterprise CA certificate with an account that has certificate enrollment permissions.
2. On the offline subordinate CA computer, open Internet Explorer.
3. In **Address**, type **http://localhost/certsrv** and then press ENTER.
4. On the **Welcome** page, click **Request a certificate**.
5. On the **Request a Certificate** page, click **Advanced certificate request**.
6. On the **Advanced Certificate Request** page, click **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file** or **Submit a renewal request by using a base-64-encoded PKCS #7 file**.
7. Open a text editor, such as Notepad, and open the CorporateEnt1CA request file.
8. On the **Edit** menu, click **Select All**, and then, on the **Edit** menu, click **Copy**.
9. In Internet Explorer, on the **Submit a Certificate Request or Renewal Request** page, in **the Saved Request** box, right-click a blank space, click **Paste**, and then click **Submit**.

   The request is submitted to the CA and remains in the Pending Requests folder. Note the request ID number and the time that are supplied by the Web page. This information is helpful when you use the procedure to approve the request (by request number) and retrieve the certificate (by request time).

10. Click **Home**.

Note A request must be retrieved by the same user account on the same computer from which it was submitted. The Web page uses a browser cookie to identify the pending request. If browser cookies are blocked or if you use a different computer, retrieve the certificate directly from the CA by using the Certification Authority MMC snap-in. For more information, see "Export the offline intermediate certificate at the root CA" in this document.

To Issue the Pending Request With the Certification Authority MMC

1. Open the Certification Authority MMC.

2. In the console pane, double-click **Certification Authority (***LocationOfCA***)**, double-click the CA, and then click **Pending Requests**.
3. In the details pane, right-click the request, and then click **Issue**.

To Issue the Pending Request Through Web Enrollment Support

1. Open Internet Explorer.
2. In **Address**, type **http://localhost/certsrv** and then press ENTER.
3. On the **Welcome** page, **click View the status of a pending certificate request**.
4. On the **View the Status of a Pending Certificate Request** page, click the request you want to issue.

   If there is more than one certificate available, click the certificate that corresponds to the time that you sent the request to the CA.
5. On the next page, choose a format for the newly issued certificate.

   In a homogenous Windows environment, it is recommended that you use the DER-encoded format.

   Unless the root CA has been previously installed on the computer account where the enterprise CA is installed (Group Policy, and so on), the root CA certificate must be trusted before the enterprise subordinate CA can start.
6. Click **Download certificate chain**, save the output to a .p7b file, and then save the file on a floppy disk.

   For example, you can save the file as CorporateEntCA.p7b.

Note There is no sensitive data on the floppy disk. A CA certificate is public information, however, the associated CA private key has been generated in the CA (or HSM). The private key does not leave the computer on which the certificate request was created.

Verify the EnterpriseSub1CA Certificate

To ensure that the certificate that you issued for the CorporateEnt1CA computer has the correct certificate properties, you should verify the certificate. Open the certificate and examine its certificate properties. To view the certificate, double-click the certificate file in Windows Explorer or use the Certificate Manager MMC. Make sure that the validity time, the key length, and certificate policies are shown correctly.

Install the Certificate at the CorporateEnt1CA Computer

The installation procedure for the enterprise CA certificate is very similar to the installation procedure for the IntermediateCA1 computer.

- Insert the floppy disk that has the certificate file for the parent CA certificates into the floppy disk drive, and then, at a command prompt, type the following command, and then press ENTER:

  certutil.exe –installcert *CACertFile***.p7b**

For more information, see "Install the certificate at IntermediateCA1 at a command prompt," later in this paper.

Verify the CorporateEnt1CA Trust Chain

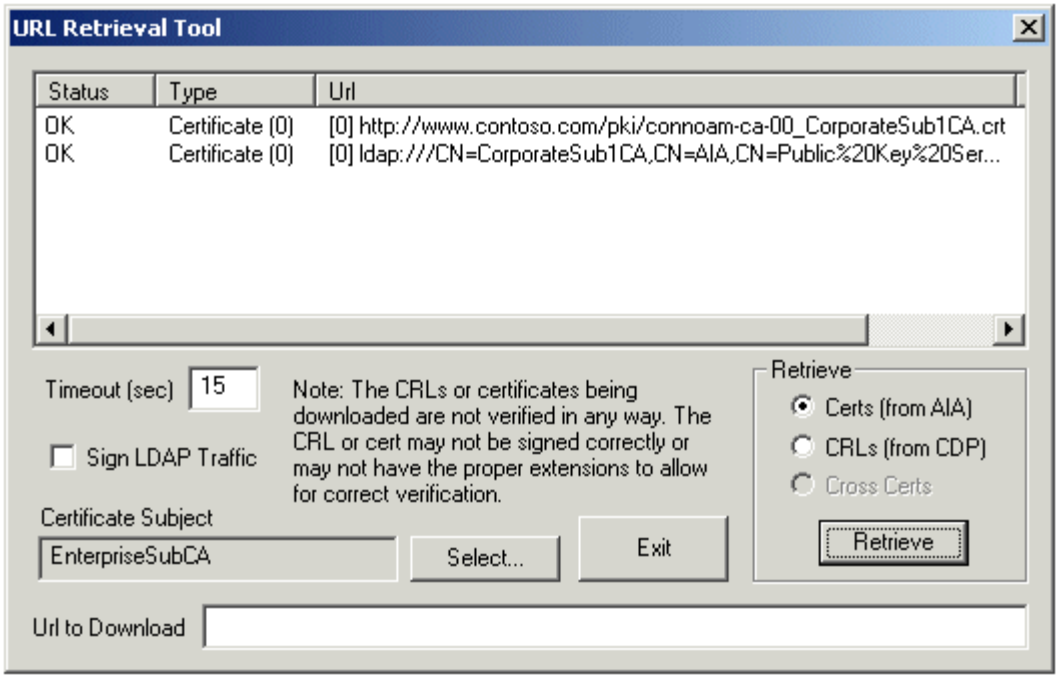
Only a valid trust chain ensures that the CA will operate as expected. If the trust chain is not correct or if the issuing CA cannot build the chain and check revocation status of parent certificates, the issuing CA will report and error when attempting to start. If the CA certificate verification fails, the following error message appears: "The revocation function was unable to check revocation because the revocation server was offline (0x80092013)."

To verify the trust chain of the CorporateEnt1CA computer in advance, at a command prompt, type **run certutil –verify** *CertificateName***.crt**, and then press ENTER.

It is also recommended that you validate the CA certificate's CRL distribution points. To do this, at a command prompt, type the following command, and then press ENTER:

certutil –URL certificate-name.crt

The output of the script looks similar to the following figure:



If your browser does not support inline frames, click here to view on a separate page.

Figure 9 Validated CRL Distribution Points

To view the CRL, in the **Url** column, double-click the CRL URL.

> **Note** You can verify a CRL or AIA according to the URL that is specified in a certificate. If a certificate and a URL are both provided, the CRLs and AIAs for all URLs that are specified in the certificate are requested and, additionally, the information from the location that is specified in **URL to download** is received.

For troubleshooting purposes, you may also be required to download the CRL to the local computer to examine the CRL. This procedure is easy for CRLs that you can gain access to by using HTTP, but this procedure is more difficult for CRLs that do have only an LDAP CRL distribution point.

You can download a binary copy of a CRL from an LDAP CRL distribution point by using the **Certutil.exe** command. To do this, type the following at a command prompt: Note that you should replace the items that are in italic text with your CRL destination and that you should verify that the correct search filter is added after the question mark.

certutil –store –split
"ldap:///CN=*CorporateRootCA***,CN=***RootCA***,CN=CDP,CN=Public Key Services,CN=Services,CN=Config**
CertificateRevocationList?base?objectClass=cRLDistributionPoint"**

After you run the command, a new CRL file is available in the directory you used when you ran the **Certutil.exe** command. The file is named Blob0_0.crl. You can open the .crl file through Windows Explorer and display it as you would any other .crl file.

PKI Health Tool

You can also use the PKI Health tool (Pkiview.msc) to verify the CRL and AIA location. This tool is available in the Windows Server 2003 Resource Kit or from the Microsoft Windows Deployment and Resource Kits Web site.

The PKI Health tool is of value to CA administrators who maintain the enterprise. The tool enumerates all certification authorities (CAs) that are associated with the current forest, and then the tool displays status properties that are associated with those CAs.

Configure the Enterprise Online CA

The CorporateEnt1CA computer configuration is similar to the parent subordinate CA configuration, and you can quickly create this configuration with a batch script. The difference between the parent CA configuration and the CorporateEnt1CA computer configuration is the validity period for issued certificates—they are controlled by templates in the enterprise CA instead of by the registry. Further, delta CRLs are enabled for the enterprise CA. Delta CRL publishing is enabled by default with Windows 2003 Server. To configure the

enterprise CA:

1. Open Notepad.
2. In this paper, go to "Sample script to configure the EnterpriseSubCA" and copy the script to the clipboard.
3. In Notepad, paste the script into a new file.
4. Save the file as **%temp%\entcacfg.cmd**, and then close Notepad.
5. At a command prompt, type **%temp%\entcacfg.cmd** and press ENTER.

Important If you study the script that configures the enterprise CA, you may notice that the **LDAP CRL publication** property is different than the properties for the offline CAs. This behavior occurs because an online CA has the capability to publish its CA certificate and the CRL automatically to Active Directory. Therefore, it is recommended that you allow the CA to update the information that is stored at the CRL and AIA distribution point. An offline CA cannot use this setting, because it cannot reach a domain controller by using the network. Because of this, no publication is configured for either CRL or AIA CRL distribution points that are configured with offline CAs.

Verify the EnterpriseSubCA Configuration

The next sections help you ensure that the CA is correctly configured and is ready for production operations. It is recommended that you apply the verification steps that are described in the previous sections in this document:

- Verify the root CA configuration
- Verify the CorporateRootCA CRL and AIA configuration
- Verify the published CRL

An enterprise CA automatically publishes the CA certificate and CRL into Active Directory. Because of this, you should also verify the CRL's availability in Active Directory. It is recommended that you use the **certutil –URL** command or the PKI Health tool that is described in the previous section.

Note The output samples that are mentioned in the previous sections in this document are not the same as the IntermediateCA1 configuration. Verify the appropriate parameters according to the EnterpriseSubxCA configuration.

Certification Authority Maintenance

CA maintenance and monitoring is an ongoing task after you set up the CA environment.

Some of the most important procedures for CA maintenance are:

- Correct configuration of the CAs
- CRL publication of offline CAs
- CRLs that are not manually published
- Renewal of CA certificates assigned to CA operations
- Backup and recovery

You can maintain the CA that is connected to the network locally or you can maintain the CA that is connected to the network through a remote connection; however, CA maintenance and administration tools are designed to work best for local operations because the CA administration is a sensitive operation and should be kept as secure as possible.

If you want to use the Certificate Services MMC for remote administration, for the appropriate steps to make the CA remotely accessible, see "Users Allowed to Manage the CA Cannot Access It Remotely" in the Microsoft Knowledge Base.

For more information on CA operations and custom configuration, refer to the Windows Server 2003 PKI Operations Guide on the Microsoft Web site.

Best Practices for CRL Publication

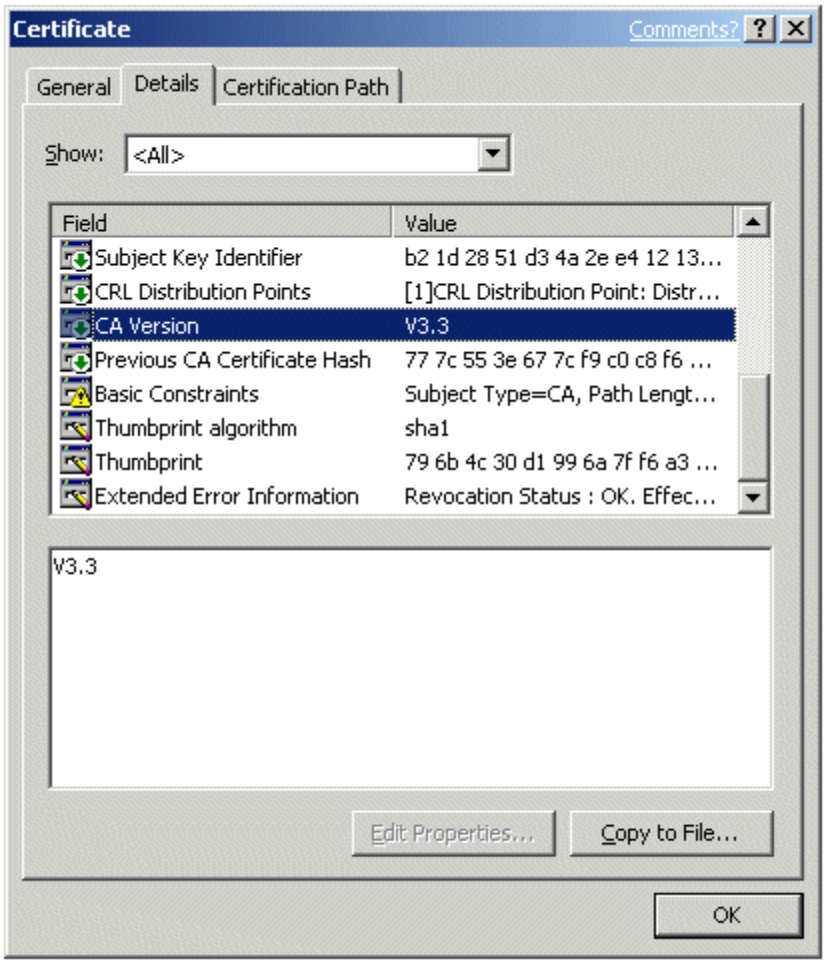
The following section provides information and best practices for managing and publishing certificate revocation lists.

CRL Partitioning

Administrators may renew an issuing CA with a new key to partition the CRL. When a new key and certificate are generated, the CA uses the new key as well as any unexpired previous keys that correspond to previous certificates when generating revocation information. Therefore, a CA may be using multiple keys at the same time and therefore publishes multiple CRLs that correspond to those keys. You can see multiple valid certificates that are assigned to the CA in the Certification Authority MMC if you click the General tab of the CA

properties.

You can also determine the renewal status of the CA if you examine the CA certificate. The CA version extension identifies how many times a CA has been renewed and how many times it has been renewed with a new key. The following figure displays a CA certificate that has been renewed three times. Note that a new key was issued with each renewal, which is why **CA Version** is 3.3.



If your browser does not support inline frames, click here to view on a separate page.

Figure 10 Renewed CA Certificate

After a CA is renewed with a new key, only the new key is used when signing new certificates. The unexpired previous keys continue to be used to sign CRLs for certificates that were signed with the previous keys. Therefore, a CA may publish multiple CRLs at the same time, each using a different key. This method of CA renewal may be an ideal method for CRL size control and effective CRL partitioning with the CA.

Automatic Root CA Cross-Certificate Generation

On computers that are running a member of the Windows Server 2003 family, Microsoft root CAs can automatically issue and publish cross certificates for a root CA that has been renewed. For example, when a Windows Server 2003 root CA is renewed with a new key, the root CA cross-certifies the renewed root CA certificate and it is considered a qualified subordinate to the earlier root CA certificate. This functionality is important if you have an operational root CA that is trusted by other organizations' clients, bridge CAs, or if it is cross-certified by other organizations.

To force the root CA to use the CrossCA certificate template, at a command prompt, type the following command, and then press ENTER. If you do not use this command without this setting configured, the CA does not use the CrossCA certificate template (even if it is available). Instead, it generates a certificate using predefined extensions in the registry:

certutil -setreg ca\CRLFlags +CRLF_USE_CROSS_CERT_TEMPLATE

To disable automatic cross CA certificate generation, at a command prompt, type the following command, and then press ENTER:

certutil -setreg ca\CRLFlags +CRLF_DISABLE_ROOT_CROSS_CERTS

To force the root CA to use the CAExchange certificate template when generating CA encryption certificates on demand, use the following command. Without this flag, the CA uses the CAExchange certificate template, when available, and generates a certificate without the template by using pre-defined extensions.

certutil -setreg ca\CRLFlags +CRLF_USE_XCHG_CERT_TEMPLATE

Certification Authority Backup and Recovery

The CA stores information about certificates in its database and the log files that are bound to the database. The CA has to be able to gain access to its certificates and keys that are stored in the local computer's certificate store or on an hardware device. CA configuration information is stored in the registry.

You can back up the database and the log files only by using the **certutil –backup** command. You can individually back up the CA certificate and the keys by using the **certutil –backupkey** command. You can archive the database by using the **certutil –backupdb** command. These backup procedures are appropriate for a restore operation that repairs a damaged CA, assuming that the CA is correctly configured. However, neither of these commands will back up any of the CA configuration or role separation information in the registry. To back up the CA, including its configuration, use the **ntbackup backup systemstate** command.

Note Backing up a CA includes the private key that is owned by the CA. The private key is the most sensitive CA information option. It becomes part of your backup data if you run **certutil -backupkey** or if you perform a system state backup. Handle the backup data with caution at all times. Store it securely if the private CA key is part of your backup. The organization's certificate policy and security policy must cover the handling of backup media.

A backup procedure may not work as expected, so it is recommended that regularly scheduled tests of restore operations be performed. For more information on CA backup, see the following Microsoft Knowledge Base articles:

- "HOW TO: Back Up and Restore a Certificate Authority in Windows" on the Microsoft Knowledge Base.
- "Certificate Server Does Not Create Backups of Installed Keys" on the Microsoft Knowledge Base. (This article applies only to Windows 2000 Server.)

Repair the Certificate Store

When you restore a CA that maintains its CA certificate with a software CSP on a different computer, you must repair the CA configuration to allow the CA to gain access to the original CA certificate. When the CA software, the database, and CA configuration are restored, you need to install the CA certificate to the local computer's certificate store. You can also use the following command to share an HSM across multiple computers:

certutil -addstore my CA01.Contoso.com_CARoot.crt

After you use this command, use the following command to determine the certificate hash:

cerutil CA01.Contoso.com_CARoot.crt | findstr /c:" Key Id Hash(sha1)"

When you use this command, it displays the CACertSHA-1Hash value. Take the hexadecimal string representing the SHA-1 hash (known as the *thumbprint property* of a certificate) and use it as a parameter in the next command. For example, you might type the following command:

certutil -repairstore my "ea c7 7d 7e e8 cd 84 9b e8 aa 71 6d f4 b7 e5 09 d9 b6 32 1b"

Appendix A: Directory Objects

The various PKI-related containers such as CAs, enrollment services, templates, object identifiers (also known as OIDs), AIA, and CRL distribution points are created when you set up the forest for the first time with the first enterprise CA. The permissions on the objects are also set at that time.

Directory objects that are created by an enterprise CA

Installing an enterprise CA creates the following objects:

- Enrollment Services object (includes CA certificate) – under CN=Enrollment Services,CN=Public Key Services,CN=Services,CN=Configuration,DC=…
- Trusted root CA object (includes CA certificate) – CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configuration,DC=…
- AIA object (includes CA certificate) – under CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,DC=…
- KRA object (no significantly sized attributes) (Windows Server 2003 only) – under CN=KRA,CN=Public Key Services,CN=Services,CN=Configuration,DC=…
- CRL distribution point container (no significantly sized attributes) – under CN=CDP,CN=Public Key

Services,CN=Services,CN=Configuration,DC=…

- CRL distribution point object (includes CRL) – under = CN=Computer,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=…?

The installation procedure also adds the CA certificate to the following existing object to provide trust for logon and authentication certificates:

- Trusted Enterprise CA certificates – CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration,DC=…

Directory Objects That Are Created by the First Enterprise CA in the Forest

Installing the first enterprise CA in the forest also installs 29 template objects when running a member of the Windows Server 2003 family or 24 template objects when running Windows 2000 in Active Directory under the following container:

CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=…

The Windows Server 2003 family adds some additional object identifier containers (also known as OID) to the configuration container. Because object identifiers are not hardcoded in version 2 (V2) templates, object identifier containers are required to work with V2 templates. Only clients running Windows XP and later may resolve object identifiers in Active Directory to friendly names.

CN=OID,CN=Public Key Services,CN=Services,CN=Configuration,DC=…

For more information, see article 287547, "Object IDs Associated with Microsoft Cryptography" in the Microsoft Knowledge Base.

Contents of \\Localhost\CertConfig and \\Localhost\CertEnroll

Because more than one certificate file exists in the \CertConfig and \CertEnroll share after a period of time, the following table explains the certificate file name extensions and their purpose. If the CA name is used as part of a file name, the sanitized CA name adds additional escape characters in order to accommodate any extended ASCII characters in the file name. The escape characters appear in the file name as %20.

Table 21 Certificate Paths and File Name Extensions

Example of the file name	Description
\\Localhost\CertConfig\Certsrv.txt	CA configuration file
\\Localhost\CertConfig\Certsrv.bak	Previous CA configuration file if the CA has been reinstalled
\\Localhost\CertConfig*CAname***.req** **\\Localhost\CertConfig***CAname***(1).req**	Request file that is used to generate the CA certificate. Request files are used only for subordinate CAs. Request files are generated with the same base file name suffix as certificates.
*SystemDriveAndSystemroot**CAname***.req** *SystemDriveAndSystemroot**CAname***(1).req**	If no shared folder was created during the CA setup procedure and Active Directory is used to publish the CA's configuration information, request files are written to the Systemroot drive instead of to the \\Localhost\CertConfig file. To verify where the configuration information is published, at a command prompt, type **certutil –getreg CA\UseDS**. If the value is set to 0, the configuration information is written to the shared folder. If the value is set to 1, the configuration is maintained in Active Directory.)
\\Localhost\CertConfig*CAname***.crt** **\\Localhost\CertEnroll***CAname***.crt**	Original root CA certificate (V0.0)
\\Localhost\CertConfig*CAname***(1).crt** **\\Localhost\CertEnroll***CAname***(1).crt**	Renewed root CA certificate (V1.0)
\\Localhost\CertConfig*CAname***(0-1).crt**	Cross certificate for CA certificate V0.0 to V1.0

\\Localhost\CertEnroll*CAname***(0-1).crt**	
\\Localhost\CertConfig*CAname***(1-0).crt** **\\Localhost\CertEnroll***CAname***(1-0).crt**	Cross certificate for CA certificate V1.0 to V0.0
\\Localhost\CertConfig*CAname***(2).crt** **\\Localhost\CertEnroll***CAname***(2).crt**	renewed root CA cert (V2.0)
\\Localhost\CertEnroll*CAname***.crl**	CA base revocation list
\\Localhost\CertEnroll*CAname***(1).crl**	CA base revocation list (first instance)
\\Localhost\CertEnroll*Caname***+.crl**	Delta CRL
\\Localhost\CertEnroll*Caname***(1)+.crl**	Delta CRL (first instance)

The cross-certificates are automatically generated when the Certificates service starts after renewing a root CA certificate with a new key. Cross-certificates are not created for subordinate CAs, and it does not occur when a root certificate is renewed with the same key. If you upgrade from Windows 2000 Server after renewing a root CA certificate with a new key, the cross certificate is generated the first time that the certificate server service starts after you upgrade to Windows Server 2003.

The following sample is an example of \\Localhost\Certenroll after a clean root CA installation.

```
C:\>dir \\Localhost\certenroll
 Volume in drive \\Localhost\certenroll has no label.
 Volume Serial Number is CC0E-CACB

 Directory of \\Localhost\certenroll

06/12/2002  11:57 AM    <DIR>          .
06/12/2002  11:57 AM    <DIR>          ..
06/12/2002  11:32 AM             1,299 concorp-
ca-00_CorporateRootCA.crt
06/12/2002  11:32 AM               925 CorporateRootCA.crl
06/12/2002  11:32 AM               321 nsrev_CorporateRootCA.asp
               3 File(s)          2,545 bytes
               2 Dir(s)   4,478,095,360 bytes free
```

The following sample is an example of \\Localhost\Certconfig after a clean root CA installation.

```
C:\>dir \\localhost\certconfig
 Volume in drive \\localhost\certconfig has no label.
 Volume Serial Number is CC0E-CACB

 Directory of \\localhost\certconfig

06/12/2002  12:28 PM    <DIR>          .
06/12/2002  12:28 PM    <DIR>          ..
06/12/2002  11:32 AM               105 certsrv.bak
06/12/2002  11:32 AM               216 certsrv.txt
06/12/2002  11:32 AM             1,299 concorp-
ca-00_CorporateRootCA.crt
               3 File(s)          1,620 bytes
               2 Dir(s)   4,478,095,360 bytes free
```

The following sample is an example of \\Localhost\Certenroll after the two key renewals on a CA.

```
C:\>dir \\localhost\certenroll
 Volume in drive \\localhost\certenroll has no label.
 Volume Serial Number is CC0E-CACB

 Directory of \\localhost\certenroll

06/11/2002  07:48 PM    <DIR>          .
06/11/2002  07:48 PM    <DIR>          ..
06/11/2002  05:31 PM             1,338 concorp-
ca-00_CorporateRootCA(1).crt
06/11/2002  05:31 PM             1,928 concorp-ca-00_CorporateRootCA
(0-1).crt
06/11/2002  05:31 PM             1,940 concorp-ca-00_CorporateRootCA
(1-0).crt
06/11/2002  07:48 PM             1,338 concorp-
```

```
ca-00_CorporateRootCA(2).crt
06/11/2002  11:57 AM             1,299 concorp-
ca-00_CorporateRootCA.crt
06/11/2002  05:31 PM               943 CorporateRootCA(1).crl
06/11/2002  05:32 PM               938 CorporateRootCA.crl
06/11/2002  11:57 AM               321 nsrev_CorporateRootCA.asp
               8 File(s)         10,045 bytes
               2 Dir(s)   4,481,171,456 bytes free
```

The following sample is an example of \\Localhost\Certconfig after two key renewals on a CA.

```
C:\>dir \\localhost\certconfig
 Volume in drive \\localhost\certconfig has no label.
 Volume Serial Number is CC0E-CACB

 Directory of \\localhost\certconfig

06/11/2002  07:48 PM    <DIR>          .
06/11/2002  07:48 PM    <DIR>          ..
06/11/2002  11:27 AM               105 certsrv.bak
06/11/2002  11:57 AM               216 certsrv.txt
06/11/2002  05:31 PM             1,928 concorp-ca-00_CorporateRootCA
(0-1).crt
06/11/2002  05:31 PM             1,338 concorp-
ca-00_CorporateRootCA(1).crt
06/11/2002  05:31 PM             1,940 concorp-ca-00_CorporateRootCA
(1-0).crt
06/11/2002  07:48 PM             1,338 concorp-
ca-00_CorporateRootCA(2).crt
06/11/2002  11:57 AM             1,299 concorp-
ca-00_CorporateRootCA.crt
04/24/2002  10:53 AM             1,942 connoam-ca-00_CONNOAM-CA-00.req
               8 File(s)         10,106 bytes
               2 Dir(s)   4,481,171,456 bytes free
```

Relationship of the Configuration Container and Certificate Store

The table in this section describes the relationship between the information that is stored in the configuration container of Active Directory and the certificate store. Typically, parts of the configuration information are replicated to the client's certificate store.

The default view of the Certificates MMC does not display the physical structure of the certificate store. To view the physical structure of the certificate store, follow this procedure:

1. Open **Certificates**.

   To do this, click **Start**, click **Run**, in the **Open** box, type **certmgr.msc**, and then press ENTER.

2. Verify that the local computer's certificates and the current users certificate are displayed in the console tree.
3. In the console tree, click **Certificate (Local Computer)**.
4. On the **View** menu, click **Options** , and select the **Physical certificates store** check box.

   Note Any information that is stored in a registry container has an impact on only the local client. Registry containers never receive information from the Active Directory configuration context. The **Intermediate Certificate Authorities – Group Policy** container is not used in the client certificate store.

Certificates that are stored in the Active Directory Configuration container (Sites and Services) are deployed to all clients across the forest. Certificates that are deployed through domain security are deployed only in the domain. If a certificate is registered in the Configuration container and the Domain Security Group Policy object (GPO), a certificate may occur twice on the client. To prevent confusion with expired or invalid certificates, you must ensure that certificates are correctly published.

You can view the Active Directory configuration context through the Active Directory Sites and Services MMC.

Table 22 Certificate Containers and Certificate Stores

Active Directory Configuration container	**Client certificates store**
Active Directory Sites and Services MMC In the console tree, navigate to Certification Authorities:	**Local Computer** In the console tree, navigate to Certificates:

DomainName\Configuration Services\Public Key Services\Certification Authorities Enterprise CAs are installed and automatically published to this location. CA certificates may also be added manually through the **certutil –dspublish** command.	Trusted Root Certificate Authorities\Enterprise\Certificates
Sites and Services MMC In the console tree, navigate to AIA: *DomainName*\Configuration\Services\Public Key Services\AIA This container also contains qualified subordination certificates (cross-certificates) that are controlled by the template that is used to generate CA certificates.	**Local Computer** In the console tree, navigate to Certificates: Intermediate Certificate Authorities\Enterprise\Certificates Windows 2000, Windows XP, or Windows Server 2003 clients automatically download the content from the configuration container; Windows 2000 clients do not support cross-certificates
Domain Security Settings MMC In the console tree, navigate to Trusted Root Certification Authorities: Computer Configuration\Windows settings\Security Settings\Public Key Policies\Trusted Root Certification Authorities	**Local Computer** In the console tree, navigate to Certificates: Trusted Root Certificate Authorities\Group Policy\Certificates
Domain Security Settings MMC In the console tree, navigate to Enterprise Trust: Computer Configuration\Windows Settings\Security Settings\Public Key Policies\Enterprise Trust	**Local Computer** In the console tree, navigate to Group Policy: Enterprise Trust\Group Policy

Default CA Certificate and CRL Storage

During the installation of the root CA, the root certificate is saved to the following locations:

- \\Localhost\Certenroll
- \\Locahost\Certconfig
- The Certificates "MY" store of the local computer
- The Trusted Root Certification Authorities container in the local computer registry

The initial CRL is published in the following locations:

- \\Localhost\Certenroll
- The Intermediate Certification Authorities container in the registry of the local computer

The CA certificate of the stand-alone CA is stored in the following locations:

- \\Localhost\Certenroll
- \\Locahost\Certconfig
- Certificates store of the local computer. To look at the store, do one of the following:
  - In the Certificates MMC, in the console tree, double-click **Certificates (Local Computer)**, double-click **Registry**, and then click **Certificates**.
  - In the Certificates MMC, in the console tree, double-click **Certificates (Local Computer)**, double-click **Intermediate Certification Authorities**, double-click **Registry**, and then click **Certificates**.

The CRL of the root CA should be stored in the following locations:

- Certificates store of the local computer. To look at the store, do the following:
  - In the Certificates MMC, in the console tree, double-click **Certificates (Local Computer)**, double-click **Intermediate Certification Authorities**, double-click **Registry**, and then click **Certificate Revocation List**

The CRL of the stand-alone CA is stored in the following locations:

- File share \\Localhost\Certenroll
- Certificates store of the local computer. To look at the store, do the following:

- In the Certificates MMC, in the console tree, double-click **Certificates (Local Computer)**, double-click **Intermediate Certification Authorities**, double-click **Registry**, and then click **Certificate Revocation List**

Mapping Custom Object Identifiers to Friendly Names

When a certificate is enrolled and that certificate carries a custom object identifier and the policy information, an enrolled certificate's purpose may display an object identifier instead of a friendly description.

This occurs because the template that is used for certificate enrollment cannot translate the object identifier into a friendly name. Because of this, custom object identifiers are mapped to friendly names through the object identifier (also known as OID) container in the Active Directory. The mapping must be done in the V2 template that will use the custom object identifier. To translate the object identifier into a friendly name:

1. Open the Certificate Templates MMC.

   To do this, click **Start**, click **Run**, in the **Open** box, type **certtmpl.msc**, press ENTER, and then open any V2 template.
2. Click the **Extensions** tab.
3. Click the **Application Policies** extension.
4. Click **Edit**, click **Add**, and then click **New**.
5. Type both the friendly name and related object identifier number, and then click **OK**.

CAPolicy.inf Syntax

The purpose of the CAPolicy.inf configuration file and its syntax is described in Windows Server 2003 Server Help.

If a CAPolicy.inf file exists, it supersedes the default configuration that is used to install a CA or renew its CA certificate.

Sample CAPolicy.inf File for CorporateRootCA

You can use the sample in this section for the root CA's CAPolicy.inf file. Verify that the parameters in the [Certsrv_Server] section are the same as your requirements, according to the CPS.

Note The parameters specified in the [Certsrv_Server] section must be greater or must match the key length and validity period used during CA setup otherwise the value specified in the capolicy.inf will be ignored.

```
[Version]
Signature= "$Windows NT$"

[Certsrv_Server]
RenewalKeyLength=4096
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=20

[CRLDistributionPoint]

[AuthorityInformationAccess]
```

If you are using a Windows 2000 CA, see article Q297528, "CRL Distribution Point Extension Is Not Suppressed by the Capolicy.inf File," in the Microsoft Knowledge Base.

Sample CAPolicy.inf File for IntermediateCA1

This section contains a sample for the subordinate CA's CAPolicy.inf file.

The object identifiers and the URLs are provided only as an example. You should replace the object identifier values with object identifiers that belong to your organization and verify that the URLs are pointing to a location that is accessible.

The CAPolicy.inf file syntax in Windows 2000 and Windows Server 2003 are basically the same, except that the [CApolicy] section, which was valid in Windows 2000, is now [PolicyStatementExtension].

On a Windows 2000 CA, the CAPolicy.inf file should look like the following sample, except that the italicized items are placeholders. The placeholders should be replaced with the information for your specific situation.

```
[Version]
Signature= "$Windows NT$"

[CApolicy]
```

```
Policies = AllIssuancePolicy
Critical = FALSE

[AllIssuancePolicy]
OID = 2.5.29.32.0
```

For a Windows Server 2003 CA, the CAPolicy.inf file should look like the following sample, where the italicized items are placeholders.

```
[Version]
Signature= "$Windows NT$"

[PolicyStatementExtension]
Policies = AllIssuancePolicy
Critical = FALSE

[AllIssuancePolicy]
OID = 2.5.29.32.0
```

Sample CAPolicy.inf File for CorporateEnt1CA

For the Windows 2000 Family

```
[Version]
Signature= "$Windows NT$"

[CApolicy]
Policies = LegalPolicy, LimitedUsePolicy

[LegalPolicy]
OID = 1.1.1.1.1.1.1.1
URL = "http://www.contoso.com/pki/Policy/USLegalPolicy.asp"
URL = "ftp://ftp.contoso.com/pki/Policy/USLegalPolicy.txt"

[LimitedUsePolicy]
OID = 2.2.2.2.2.2.2.2
URL = "http://www.contoso.com/pki/Policy/USLimitedUsePolicy.asp"
URL = "ftp://ftp.contoso.com/pki/Policy/USLimitedUsePolicy.txt"
```

For the Windows Server 2003 Family

```
[Version]
Signature= "$Windows NT$"

[PolicyStatementExtension]
Policies = LegalPolicy, LimitedUsePolicy

[LegalPolicy]
OID = 1.1.1.1.1.1.1.1
URL = "http://www.contoso.com/pki/Policy/USLegalPolicy.asp"
URL = "ftp://ftp.contoso.com/pki/Policy/USLegalPolicy.txt"

[LimitedUsePolicy]
OID = 2.2.2.2.2.2.2.2
URL = "http://www.contoso.com/pki/Policy/USLimitedUsePolicy.asp"
URL = "ftp://ftp.contoso.com/pki/Policy/USLimitedUsePolicy.txt"
```

CRL Distribution Point Replacement Token

Replacement tokens are used to retain the configuration of distribution points flexible. You can use replacement tokens in the CAPolicy.inf file and in the Certification Authority MMC in **CA Extensions**.

A replacement token consists of the percent sign and a number. This behavior occurs if you use replacement tokens in the Certificate Services MMC or if you use them in a **certutil** command. If replacement tokens are used in a batch file, and you use the percent sign (%), you must use another escape sign when needed, because the Windows shell typically interprets a percent sign as a command-line parameter.

The mapping of replacement tokens is different in versions of Windows later than Windows 2000 Server. For more information and a list of replacement tokens that are valid on computers that are running Windows 2000, see Article 283119, "Error Message: A Replacement Token Entered Does Not Match Any Recognized Token" in the Microsoft Knowledge Base.

You can use the following tokens for **CRLDistributionPoint**, **AuthorityInformationAccess**, and **CrossCertificateDistributionPointsExtension** URLs.

Table 23 CRL Distribution Point Replacement Tokens

Token name	Description	Windows 2000 map value	Windows Server 2003 map value
ServerDNSName	The DNS name of the CA server	%1	%1
ServerShortName	The NetBIOS name of the CA server	%2	%2
CaName	The name of the CA	%3	%3
Cert_Suffix	The renewal extension of the CA	%4	N/A
CertificateName		N/A	%4
Domain_Name	The location of the domain root in Active Directory	%5	N/A
(Not used)		N/A	%5
ConfigurationContainer	The location of the configuration container in Active Directory	%6	%6
CATruncatedName	The "sanitized" name of the CA, 32 characters with a hash on the end	%7	%7
CRLNameSuffix	The renewal extension for the CRL	%8	%8
DeltaCRLAllowed			%9
CDPObjectClass			%10
CAObjectClass			%11

The Certification Server setup process replaces all **%number%** sequences with the appropriate value.

CRL Publishing Properties

The **Publish CRLs to this location** flag is used to identify the locations to which the CA should publish (or place) the physical CRLs when the CA publishes a CRL either automatically or manually. This flag specifies only where CRLs are published. It is also used by the **certutil.exe –dspublish** command when you manually publish CRLs to Active Directory. Both the **Publish CRL** and **Publish Delta CRL** flags on the **Revoked Certificates Properties** page are responsible for turning the publishing activity on and off.

The **Publish CRLs to this location** flag indicates the locations that the CA should attempt to use to publish the CRL. This flag does not configure the server to conduct the publishing activity, but only sets it up so that the CA can determine the appropriate locations to which to publish when publishing occurs. Note that actual publishing activity is governed by the **Revoked Certificates** properties.

The **Include in all CRLs** flag specifies that the Active Directory publication location should be included in the CRL itself. This information is useful for publishing offline CRLs to Active Directory by using the **Certutil.exe** tool. To use this, at a command prompt, type **certutil –dspublish**, and then press ENTER.

The **Include in CDP extension of issued certificates** flag is used by clients to find the CRL distribution point location for the CRL. You should always specify this flag unless you do not want to use client-side checking or application revocation checking for issued certificates.

The **Include in CRLs. Clients use this to find Delta CRLs** flag is used by clients to determine if a delta CRL exists and where it is located. The location may or may not be the same as the CRL location. The delta CRL location is identified in the CRL by use of the **freshestCRL** extension in the CRL object itself.

You may want to have a base CRL in an LDAP location in Active Directory and a delta CRL at an alternate HTTP location because of the differences in replication. If the delta CRL will be issued at an interval that is shorter than the replication convergence time for your forest, the delta CRL should not be published to Active Directory. In many Active Directory networks, it may take hours for Active Directory objects to fully replicate

throughout the network. For delta CRLs that may have a lifetime only of a few hours, the replication latency often means that Active Directory clients receive a delta CRL object that has already expired by the time it reaches the client. You can avoid this latency by publishing the delta CRL to an HTTP location that is serviced by fault-tolerant Web servers, where all clients can immediately retrieve a fresh delta CRL.

Table 24 CRL Publishing Properties

Display name	Description	Decimal value	Hexadecimal value
Publish CRLs to this location	Used by the CA to determine whether to publish base CRLs to this URL	1	0x00000001
Include in the CRL distribution point extension of issued certificates	Used by clients during revocation checking to find base CRL locations	2	0x00000002
Include in [base] CRLs	Used by clients during revocation checking to find delta CRL locations from base CRLs	4	0x00000004
Include in all CRLs	Not used during revocation checking. Specifies where to publish in Active Directory when publishing manually using **certutil -dspublish**. Can be used by an offline CA to specify the LDAP URL for manually publishing CRLs. Must also set the explicit configuration container in the URL or set the **DSConfigDN** value in the registry: **certutil –setreg ca\DSConfigDN "CN=…"**	8	0x00000008
		16	0x00000010
		32	0x00000020
Publish delta CRLs to this location	Used by the CA to determine whether to publish delta CRLs to this URL	64	0x00000040

AIA Publishing Properties

The table shows the publishing properties for the Authority Information Access (AIA).

Table 25 AIA Publishing Properties

Display name	Decimal value	Hexadecimal value
Include in the AIA extension of issued certificates	1	0x00000001
Include in the online certificate status protocol (OCSP) extension	2	0x00000002

Sample Script to Configure CorporateRootCA

The script in this section applies the most important configuration changes to a Windows Server 2003 CA for

the CorporateRootCA computer.

Important Because percent (%) variables are handled differently in batch files and at a command prompt, you must use two percent signs (%%) if you run this sample script from a batch file, as described. If **certutil** is called from a command prompt and not from a batch file, only use only one percent sign (%), not two percent signs (%%).

```
REM
REM CA configuration script for a Windows Server 2003 CA
REM
REM The naming context applies to the individual organization’s Active
Directory
REM configuration
REM
SET myADnamingcontext=DC=concorp,DC=contoso,DC=com
REM
REM This variable directs to the HTTP publication location that is used
for
REM the CRL and AIA publication
REM
SET myhttpPKIvroot=http://www.contoso.com/pki
REM
REM Because CRLs and CA certificates are published in the
organization’s Active
REM Directory, no specific LDAP server name is provided.
REM Set an dedicated server-name instead
REM if a known server should provide the CRLs and AIAs
REM
SET myLDAPserver=
REM
REM Map the namespace of Active Directory
REM
certutil.exe -setreg ca\DSConfigDN
"CN=Configuration,%myADnamingcontext%"
REM
REM Configure CRL and AIA CDP
REM
REM By default, Certutil creates a registry value of type REG_SZ if a
string is
REM specified as a parameter. Some registry values are expected as
REG_MULTI_SZ. To
REM create a REG_MULTI_SZ instead of a REG_SZ, add a \n to the end of
any value that
REM becomes part of the REG_MULTI_SZ
REM
certutil -setreg CA\CRLPublicationURLs
"1:%WINDIR%\system32\CertSrv\CertEnroll\%%3%%8%%9.crl\n2:%myhttp
PKIvroot%/%%3%%8%%9.crl\n10:ldap://%myLDAPserver%/CN=%%7%%8,CN=%%2,
CN=CDP,CN=Public Key Services,CN=Services,%%6%%10"
certutil -setreg CA\CACertPublicationURLs
"1:%WINDIR%\system32\CertSrv\CertEnroll\%%1_%%3%%4.crt\n2:%myhttp
PKIvroot%/%%1_%%3%%4.crt\n2:ldap://%myLDAPserver%/CN=%%7,CN=AIA,
CN=Public Key Services,CN=Services,%%6%%11"
REM
REM Configure CRL publication
REM
certutil -setreg CA\CRLPeriodUnits 180
certutil -setreg CA\CRLPeriod "Days"
REM
REM Disable Delta CRL publication
REM
certutil -setreg CA\CRLDeltaPeriodUnits 0
REM
REM Set the validity period for issued certificates
REM
certutil -setreg ca\ValidityPeriodUnits 10
certutil -setreg ca\ValidityPeriod "Years"
REM
REM Restart the CA server service
REM
net stop certsvc & net start certsvc
REM
```

```
REM Repair CA file system shares and IIS virtual roots
REM
certutil -vroot
REM
REM Republish the CRL
REM The CRL publishing may immediately not work
REM after you restart the CA server service. If this behavior
REM occurs, try the certutil –CRL command at a command
REM prompt again.
REM
certutil -CRL
REM
REM Test if CAPolicy.inf file exists
REM
IF EXIST %SYSTEMROOT%\capolicy.inf GOTO ENDCFG
ECHO “Warning, no capolicy.inf file used”
:ENDCFG
```

The following script applies the same configuration as the previous script, but it configures a Windows 2000 CA. Remember that the delta CRL configuration parameter is not supported in a Windows 2000 CA environment. To perform the **certutil –URL** and **certutil –vroot** commands, you must run the version of **certutil** that is included with Windows Server 2003 on the Windows 2000 CA computer.

```
REM
REM CA configuration script for a Windows 2000 CA
REM
REM This variable directs to the HTTP publication location that is used
for
REM the CRL and AIA publication
REM
SET myhttpPKIvroot=http://www.contoso.com/pki
REM
REM Because CRLs and CA certificates are published in the
organization’s Active
REM Directory, no specific LDAP server name is provided. Set a
dedicated server
REM name instead, if a known server should provide the CRLs and AIAs.
REM
SET myLDAPserver=
REM
REM Configure CRL and AIA CDP
REM
certutil -setreg policy\FileRevocationCRLURL "\n”
certutil -setreg policy\RevocationCRLURL
“%myhttpPKIvroot%/%%3%%8.crl\n”
certutil -setreg policy\LDAPRevocationCRLURL
“ldap://%myLDAPserver%/CN=%%7%%8,CN=%%2,CN=CDP,CN=Public Key Services,
CN=Services,%%6?certificateRevocationList?base?objectclass=
cRLDistributionPoint\n"

certutil -setreg policy\FileIssuercertURL  "\n”
certutil -setreg policy\IssuercertURL “%myhttpPKIvroot%/%%1_%%3%%4.crt"
certutil -setreg policy\LDAPIssuercertURL
“ldap://%myLDAPserver%/CN=%%7,CN=AIA,CN=Public  Key
 Services,CN=Services,%%6?cACertificate?base?objectclass=
certificationAuthority”
REM
REM Configure CRL publication
REM
certutil -setreg CA\CRLPeriodUnits 180
certutil -setreg CA\CRLPeriod "Days"
REM
REM Set the validity period for issued certificates
REM
certutil -setreg ca\ValidityPeriodUnits 10
certutil -setreg ca\ValidityPeriod "Years"
REM
REM Disable issuer name and issuer serial number
REM
certutil -setreg policy\EditFlags -EDITF_ENABLEAKIISSUERNAME
certutil -setreg policy\EditFlags -EDITF_ENABLEAKIISSUERSERIAL
REM
```

```
REM Restart the CA server service
REM
net stop certsvc & net start certsvc
REM
REM Repair CA files-system shares and IIS virtual roots
REM
certutil -vroot
REM
REM Publish the CRL with the updated CDP and naming information.
REM It might happen that CRL publishing fails immediately
REM after the CA server service has been restarted. If this
REM is the case, try certutil –CRL at a command prompt again.
REM
certutil -CRL
```

Sample Script to Configure IntermediateCA

The following script applies the most important configuration changes to a Windows Server 2003 CA for the IntermediateCA computer.

```
REM
REM CA configuration script for a Windows Server 2003 CA
REM
REM The naming context applies to the individual organization’s Active
Directory
REM configuration
REM
SET myADnamingcontext=DC=concorp,DC=contoso,DC=com
REM
REM This variable directs to the HTTP publication location that is used
for
REM the CRL and AIA publication
REM
SET myhttpPKIvroot=http://www.contoso.com/pki
REM
REM Because CRLs and CA certificates are published in the
organization’s Active
REM Directory, no specific LDAP server name is provided. Set an
dedicated server
REM name instead, if a known server should provide the CRLs and AIAs.
REM
SET myLDAPserver=
REM
REM Map the namespace of Active Directory
REM
certutil.exe -setreg ca\DSConfigDN
"CN=Configuration,%myADnamingcontext%"
REM
REM Configure CRL and AIA CDP
REM
REM By default, Certutil creates a registry value of type REG_SZ if a
string is
REM specified as a parameter. Some registry values are expected as
REG_MULTI_SZ.
REM To create a REG_MULTI_SZ instead of a REG_SZ, add a \n to the end
of any value
REM that becomes part of the REG_MULTI_SZ
REM
certutil -setreg CA\CRLPublicationURLs
"1:%WINDIR%\system32\CertSrv\CertEnroll\%%3%%8%%9.crl\n2:%myhttp
PKIvroot%/%%3%%8%%9.crl\n10:ldap://%myLDAPserver%/CN=%%7%%8,CN=%%2,
CN=CDP,CN=Public Key Services,CN=Services,%%6%%10"
certutil -setreg CA\CACertPublicationURLs
"1:%WINDIR%\system32\CertSrv\CertEnroll\%%1_%%3%%4.crt\n2:%myhttp
PKIvroot%/%%1_%%3%%4.crt\n2:ldap://%myLDAPserver%/CN=%%7,CN=AIA,
CN=Public Key Services,CN=Services,%%6%%11"
REM
REM Configure CRL publication
REM
certutil -setreg CA\CRLPeriodUnits 30
certutil -setreg CA\CRLPeriod "Days"
REM
```

```
REM Disable Delta CRL publication
REM
certutil -setreg CA\CRLDeltaPeriodUnits 0
REM
REM Set the validity period for issued certificates
REM
certutil -setreg ca\ValidityPeriodUnits 5
certutil -setreg ca\ValidityPeriod "Years"
REM
REM Include certificate policies in certificate request
REM
certutil -v -setreg policy\EnableRequestExtensionlist "+2.5.29.32"
REM
REM
REM Disable issuer name and issuer serial number
REM
certutil -setreg policy\EditFlags -EDITF_ENABLEAKIISSUERNAME
certutil -setreg policy\EditFlags -EDITF_ENABLEAKIISSUERSERIAL
REM
REM Restart the CA server service
REM
net stop certsvc & net start certsvc
REM
REM Repair CA files-system shares and IIS virtual roots
REM
certutil -vroot
REM
REM Republish the CRL
REM It might happen that CRL publishing fails immediately
REM after the CA server service has been restarted. If this
REM is the case, try certutil –CRL at a command prompt again.
REM
certutil -CRL
```

The following script applies the same configuration as the previous script but the following script configures a Windows 2000 CA. Remember that the delta CRL configuration parameter is not supported in a Windows 2000 CA environment. To use the **certutil –URL** and **certutil –vroot** command, you must run the Windows Server 2003 version of the **certutil** utility on the Windows 2000 CA computer.

```
REM
REM CA configuration script for a Windows 2000 CA
REM
REM This variable directs to the HTTP publication location that is used
for
REM the CRL and AIA publication
REM
SET myhttpPKIvroot=http://www.contoso.com/pki
REM
REM Because CRLs and CA certificates are published in the
organization’s Active
REM Directory, no specific LDAP server name is provided. Set a
dedicated server
REM name instead if a known server should provide the CRLs and AIAs.
REM
SET myLDAPserver=
REM
REM Configure CRL and AIA CDP
REM
REM By default, certutil creates a registry value of type REG_SZ if a
string is
REM specified as a parameter. Some registry values are expected as
REG_MULTI_SZ. To
REM create a REG_MULTI_SZ value instead of a REG_SZ value, add \n to
the end of any
REM value that becomes part of REG_MULTI_SZ.
REM
certutil -setreg policy\FileRevocationCRLURL “\n”
certutil -setreg policy\RevocationCRLURL
“%myhttpPKIvroot%/%%3%%8.crl\n”
certutil -setreg policy\LDAPRevocationCRLURL
“ldap://%myLDAPserver%/CN=%%7%%8,CN=%%2,CN=CDP,CN=Public Key Services,
CN=Services,%%6?certificateRevocationList?base?objectclass=
```

```
cRLDistributionPoint\n"

certutil -setreg policy\FileIssuercertURL
"%WINDIR%\system32\CertSrv\CertEnroll\%%1_%%3%%4.crt\n”
certutil -setreg policy\IssuercertURL “%myhttpPKIvroot%/%%1_%%3%%4.crt"
certutil -setreg policy\LDAPIssuercertURL
“ldap://%myLDAPserver%/CN=%%7,CN=AIA,CN=Public
Key Services,CN=Services,%%6?cACertificate?base?objectclass=
certificationAuthority”
REM
REM Configure CRL publication
REM
certutil -setreg CA\CRLPeriodUnits 30
certutil -setreg CA\CRLPeriod "Days"
REM
REM Set the validity period for issued certificates
REM
certutil -setreg ca\ValidityPeriodUnits 5
certutil -setreg ca\ValidityPeriod "Years"
REM
REM Include certificate policies in certificate request
REM
certutil -v -setreg policy\EnableRequestExtensionlist "+2.5.29.32"
REM
REM
REM Disable issuer name and issuer serial number
REM
certutil -setreg policy\EditFlags -EDITF_ENABLEAKIISSUERNAME
certutil -setreg policy\EditFlags -EDITF_ENABLEAKIISSUERSERIAL
REM
REM Restart the CA server service
REM
net stop certsvc & net start certsvc
REM
REM Repair CA files-system shares and IIS virtual roots
REM
certutil -vroot
REM
REM Republish the CRL.
REM It might happen that CRL publishing fails immediately
REM after the CA server service has been restarted. If this
REM is the case try certutil –CRL at a command prompt again.
REM
certutil -CRL
```

Sample Script to Configure the EnterpriseSubCA

The following script applies the most important configuration changes to a Windows Server 2003 CA for the EnterpriseSubCA computer.

> **Important** Because percent (%) variables are handled differently in batch files and at a command prompt, you must use two percent signs (%%) if you run this sample script from a batch file, as described. If **certutil** is called from a command prompt and not from a batch file, only use one percent sign (%), not two (%%).

```
REM
REM CA configuration script for a Windows Server 2003 CA
REM
REM This variable directs to the HTTP publication location that is used
for
REM CRL and AIA publication
REM
SET myhttpPKIvroot=http://www.contoso.com/pki
REM
REM Because CRLs and CA certificates are published in the
organization's Active
REM Directory, no specific LDAP server name is provided.
REM
SET myLDAPserver=
REM
REM Configure CRL and AIA CDP
REM
```

```
certutil -setreg CA\CRLPublicationURLs "65:
%WINDIR%\system32\CertSrv\CertEnroll\%%3%%8%%9.crl\n6:%myhttp
PKIvroot%/%%3%%8%%9.crl\n79:ldap://%myLDAPserver%/CN=%%7%%8,CN=%%2,
CN=CDP,CN=Public Key Services,CN=Services,%%6%%10"

certutil -setreg CA\CACertPublicationURLs  "1:
%WINDIR%\system32\CertSrv\CertEnroll\%%1_%%3%%4.crt
n2:%myhttpPKIvroot%/%%1_%%3%%4.crt\n2:ldap://%myLDAPserver%/CN=%%7,
CN=AIA,CN=Public Key Services,CN=Services,%%6%%11\"
REM
REM Configure CRL publication
REM
certutil -setreg CA\CRLPeriodUnits 1
certutil -setreg CA\CRLPeriod "Days"
REM
REM Disable issuer name and issuer serial number
REM
certutil -setreg policy\EditFlags -EDITF_ENABLEAKIISSUERNAME
certutil -setreg policy\EditFlags -EDITF_ENABLEAKIISSUERSERIAL
REM
REM Restart the CA server service
REM
net stop certsvc & net start certsvc
REM
REM Create Web virtual roots and file shares
REM
certutil.exe -vroot
REM
REM Republish the CRL
REM
certutil -CRL
```

The following script applies the same configuration as the previous script, but it configures a Windows 2000 CA. Remember that the delta CRL configuration parameter is not supported in a Windows 2000 CA environment. To use the **certutil –URL** and **certutil –vroot** commands, you must run the version of the **Certutil.exe** utility that is included with the Windows Server 2003 operating system on the computer serving as the Windows 2000 CA.

```
REM
REM CA configuration script for a Windows 2000 CA
REM
REM This variable directs to the HTTP publication location that is used
for
REM the CRL and AIA publication
REM
SET myhttpPKIvroot=http://www.contoso.com/pki
REM
REM Because CRLs and CA certificates are published in the
organization's Active
REM Directory, no specific LDAP server name is provided. Set a
dedicated server
REM name instead if a known server should provide the CRLs and AIAs.
REM
SET myLDAPserver=
REM
REM Configure CRL and AIA CDP
REM
certutil -setreg policy\FileRevocationCRLURL "\n”
certutil -setreg policy\RevocationCRLURL
“%myhttpPKIvroot%/%%3%%8.crl\n”
certutil -setreg policy\LDAPRevocationCRLURL
“ldap://%myLDAPserver%/CN=%%7%%8,CN=%%2,CN=CDP,CN=Public Key Services,
CN=Services,%%6?certificateRevocationList?base?objectclass=
cRLDistributionPoint\n"

certutil -setreg policy\FileIssuercertURL
"%WINDIR%\system32\CertSrv\CertEnroll\%%1_%%3%%4.crt\n”
certutil -setreg policy\IssuercertURL “%myhttpPKIvroot%/%%1_%%3%%4.crt"
certutil -setreg policy\LDAPIssuercertURL
“ldap://%myLDAPserver%/CN=%%7,CN=AIA,CN=Public Key
Services,CN=Services,%%6?cACertificate?base?objectclass=
certificationAuthority”
```

```
REM
REM Configure CRL publication
REM
certutil -setreg CA\CRLPeriodUnits 1
certutil -setreg CA\CRLPeriod "Days"
REM
REM Disable delta CRL publication
REM
certutil -setreg CA\CRLDeltaPeriodUnits 0
REM
REM Disable issuer name and issuer serial number
REM
certutil -setreg policy\EditFlags -EDITF_ENABLEAKIISSUERNAME
certutil -setreg policy\EditFlags -EDITF_ENABLEAKIISSUERSERIAL
REM
REM Restart the CA server service
REM
net stop certsvc & net start certsvc
REM
REM Create Web virtual roots and file shares
REM
certutil.exe -vroot
REM
REM Republish the CRL
REM
certutil -CRL
```

Appendix B: Parameters for a Three-Tier CA Topology

This section describes all of the parameters that are required to set up a three-tier CA topology. It is recommended that the values are agreed between the departments in the organization (IT department, legal department, and so on).

The parameters in this section are in the sequence in which they are used during the setup. The heading describes the parameter's name and the table contains detailed information about the parameter.

> **Important** Make sure that you have predefined all of the parameters in this section, because every value is mandatory.

Root CA Configuration Parameters

This section provides a list of parameters that must be defined during the setup procedure for a stand-alone offline root CA. The sample values are related to the sample configuration that is explained in the previous section.

Registry references follow the syntax that is used by the **certutil** command. To get more information about the registry values, at a command prompt, type **certutil –getreg -?** and press ENTER.

Renewal Key Length (CA Certificate)

Description	It is recommended that the key length does not exceed 4096 bits because this is the maximum interoperable key length with most programs and PKI providers. The renewal key length must not be shorter than the key length that you chose during the CA installation procedure.
Sample value	4096
Defined at	CAPolicy.inf
Stored at	Renewed CA certificate
Impacts	The root CA key material

Renewal Validity Period (CA Certificate)

Description	Describes the lifetime of a CA certificate that is a renewal of a previous CA certificate. It is recommended that root CAs be configured with a longer lifetime than any other CA in the hierarchy. because this configuration reduces administrative burden that is caused by renewing all certificates that are singed by the CA’s certificate.
Sample value	1020
Defined at	CAPolicy.inf

Stored at	CA certificate that is related to the date and time when the certificate was enrolled
Impacts	The CA root certificate and all certificates that will be signed by the root

Renewal Validity Period Units (CA Certificate)

Description	Defines the measurement related to the validity time. Valid values are years, months, or days. For a CA certificate lifetime the usual unit is years.
Sample value	Years
Defined at	CAPolicy.inf
Stored at	CA certificate related to the date and time when the certificate has been enrolled
Impacts	The CA root certificate and all certificates that will be signed by the root

Certificate Revocation List (CRL) Distribution Point (CA certificate)

Description	A CRL distribution point must not be configured to be contained in the self-signed root CA certificate. Most applications do not check revocation on root CA certificates; therefore, CRL distribution point extensions are not necessary or recommended. It is also senseless to set an CRL distribution point for a root certificate because there is no higher instance that could revoke the root certificate.
Sample value	None
Defined at	CAPolicy.inf
Stored at	CA certificate
Impacts	The attribute setting in the CA root certificate and all applications that verify the root CA's validity

Authority Information Access (AIA) (CA certificate)

Description	An AIA must not be specified for a root CA certificate. This is because the AIA points to the location of the certificate that was used for signing this certificate. Since a root CA is self-signed, you do not need to specify an AIA.
Sample value	None
Defined at	CAPolicy.inf
Stored at	CA certificate
Impacts	All applications that verify the root CA's validity

CSP (CA Certificate)

Description	The CSP is responsible for generating the certificate's key material and the certificate generation.
Sample value	Microsoft Strong Cryptographic Provider
Defined at	CA Installation Wizard
Stored at	For the Windows 2000 Server family and the Windows Server 2003 family: CA Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration *CAName*\CSP\Provider**
Impacts	CA certificate

Hash Algorithm

Description	Defines the hash algorithm that is used for hashing and signing certificate contents.
Sample value	SHA-1

Defined at	CA installation wizard
Stored at	CA registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration***CAName* **\CSP\HashAlgorithm**
Impacts	CA certificate

Key Length (CA Certificate)

Description	Defines the complexity of the key material assigned to the CA certificate. It is recommended that the key length does not exceed 4096 bits because this is the maximum interoperable key length today with most applications and PKI providers.
Sample value	4096
Defined at	CA Installation Wizard
Stored at	Certificate request and is only used temporarily
Impacts	The Root CA key material that could be stored within a HSM or encrypted on the CA's hard drive

Common Name

Description	The common name must not exceed 64 characters in length. It is important to remember that each space in the name will actually use three characters in the total length because of how escape characters are written (%20).
Sample value	CorporateRootCA
Defined at	CA Installation Wizard
Stored at	Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration** *CAName***CommonName**
Impacts	The common name becomes part of the certificate issuer name and is also part of the CRL and AIA if replacement tokens are used. The common name is used by several variables that are used to set the CRL and AIA.

Distinguished Name Suffix

Description	The name maps to the namespace that is used by the domain where the CA belongs to. Since the Root-CA is configured as a stand-alone CA, the distinguished name should be mapped to the same namespace that will be used for the enterprise CA.
Sample value	DC=concorp,DC=contoso,DC=com
Defined at	CA configuration that takes place after the installation
Stored at	Windows 2000 and Windows 2003 Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration** *CAName***DSConfigDN**
Impacts	The distinguished name becomes part of the certificate issuer name and is also part of the CRL and AIA if replacement tokens are used. It is also used by several variables that are used to set the CRL and AIA.

Validity Period (CA Certificate)

Description	The parameter defines how long from now the CA certificate will be valid, depending on the validity period units
Sample value	1020
Defined at	CA Installation Wizard
Stored at	CA certificate related to the date and time when the certificate has been enrolled

Impacts	The CA certificate and the validity time of all certificates that are signed by the Root CA certificate.

CA Database Path

Description	Defines where the CA's database is located in the root CA's file system.
Sample value	C:\Certlog
Defined at	CA installation wizard
Stored at	Windows 2000 and Windows 2003 Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration** *CAName***DBDirectory**
Impacts	The CA must be able to get the appropriate path name from the registry when the CA starts up.

CA Log File Path

Description	Defines where the CA's transaction log-files are located in the CA's file system.
Sample value	C:\Certlog
Defined at	CA Installation Wizard
Stored at	Windows 2000 and Windows 2003 Server families: Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration** *CAName* **\DBLogDirectory**
Impacts	The CA must be able to get the appropriate path name from the registry when the CA starts up.

Shared Folder

Description	Defines where the CA's transaction log-files are located in the root CA's file system.
Sample value	\\[{localhost]}\CertConfig
Defined at	CA installation wizard
Stored at	Windows 2000 and the Windows 2003 Server family Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration ***CAName***\ConfigurationDirectory**
Impacts	Clients, those are not able to receive the CA certificate through group policies and need to import the certificate manually.

Certificate Revocation List (CRL) Distribution Point

Description	Defines the URLs where the client will find the certificate revocation list that is related to the certificate. The CRL distribution point of a root CA should be empty.
Sample value	[empty]
Defined at	Certification Authority MMC
Stored at	Windows 2000 Server family: Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Policy \FileRevocationCRLURL** Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration \Policy\LDAPRevocationCRLURL** Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration \Policy\RevocationCRLURL**

	Windows Server 2003: Registry: **HKLM\System\CurrentControlSet\Services\CertSvc \Configuration** *CAName***CRLPublicationURLs**
Impacts	Any user, computer, service, or program that verifies the root certificate

Authority Information Access (AIA)

Description	Defines the URLs where the client can locate the certificate's issuer certificate. Because a root CA issues the CA certificate to itself, you do not need to specify an issuer. The AIA of a root CA should be empty.
Sample value	[empty]
Defined at	Certification Authority MMC
Stored at	Windows2000 Server family: Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration\Policy \FileIssuerCertURL** Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration\Policy \LDAPFileIssuerCertURL** Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration\Policy\IssuerCertUR** Windows Server 2003: Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration** *CAName***CACertPublicationURLs**
Impacts	Any user, computer, service, or program that verifies the root certificate

CRL Publication Interval

Description	The value controls the CRL validity time and the CRL publication cycle. According to the value, the CRL is published on a regular basis. Its validity time is set to the publication time and date and the defined value.
Sample value	180 days
Defined at	Certification Authority MMC
Stored at	Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration\CAName \CRLperiod** Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration\CAName \CRLperiodUnits**
Impacts	CA CRL publication algorithm and any user, computer, service, or program that verifies the CRL..

Delta CRL Publication Interval

Description	Defines similar to the CRL publication interval and the publication interval of the delta CRL. For an offline CA, it is recommended that you disable delta CRL publication.
Sample value	0 (which is equal to disabled delta CRL publication)
Defined at	Certification Authority MMC
Stored at	Windows 2000: Not available Windows Server 2003 Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration** *CAName***CRLDeltaPeriod** Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration**

	*CAName***CRLDeltaPeriodUnits**
Impacts	Any client that can verify the certificate validity through delta CRLs

Validity period

Description	Defines the period of time that a certificate that was issued by the CA is valid. The validity period cannot extend the certificate validity beyond the certificate of the issuing CA.
Sample value	5 years
Defined at	Certification Authority MMC
Stored at	Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration***CA Name***\ValidityPeriodUnits** Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration***CA Name***\ValidityPeriod**
Impacts	The validity time of any certificate that will be issued from that stand-alone CA.

Intermediate CA Configuration Parameters

This section provides a list of parameters that must be defined during the setup procedure for a stand-alone offline root CA. The sample values are related to the sample configuration that is explained in the previous section.

CA Policy

Description	Defines the URL or the text that applies to the CA's policy. The policy describes different types of rules, such as how the CA is operated, which legal policies are valid, and so on.
Sample value	OID = 1.1.1.1.1.1.1.1.1 URL = http://www.contoso.com/pki/Policy/USLegalPolicy.asp URL = "ftp://ftp.contoso.com/pki/Policy/USLegalPolicy.txt"
Defined at	CAPolicy.inf
Stored at	CA certificate
Impacts	All certificates that are directly or indirectly signed by this CA certificate

CSP (CA Certificate)

Description	Generates the certificate's key material and the certificate generation.
Sample value	Microsoft Strong Cryptographic Provider
Defined at	CA installation wizard
Stored at	CA Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration ***CAName***\CSP\Provider**
Impacts	CA certificate

Hash Algorithm

Description	Defines the hash algorithm that is used for hashing and signing certificate contents.
Sample value	SHA-1
Defined at	CA Installation Wizard
Stored at	CA registry: *CAName***\CSP\HashAlgorithm**
Impacts	CA certificate

Key Length (CA Certificate)

Description	Defines the complexity of the key material that is assigned to the CA certificate. It is

	recommended that the key length does not exceed 4096 bits, because this is the maximum interoperable key length with most applications and PKI providers. The key length of a subordinate CA is typically shorter than the key length of its parent CA.
Sample value	2048
Defined at	CA Installation Wizard
Stored at	Certificate request and is only temporarily used
Impacts	The root CA key material that could be stored in an HSM or encrypted on the CA's hard disk

Common Name

Description	The common name must not exceed 64 characters in length. It is important to remember that each space in the name uses three characters in the total of the overall length because of the escape character sequence (%20).
Sample value	IntermediateCA
Defined at	CA Installation Wizard
Stored at	Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration** *CAName***CommonName**
Impacts	The common name becomes part of the certificate issuer name and is also part of the CRL and AIA if replacement tokens are used. The common name is used by several variables that are used to set the CRL and AIA.

CA Database Path

Description	Defines where the CA's database is located in the CA's file system.
Sample value	C:\Certlog
Defined at	CA Installation Wizard
Stored at	Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration \DBDirectory**
Impacts	The CA must be able to obtain the appropriate path name from the registry when the CA starts.

CA Log File Path

Description	Defines where the CA's transaction log files are located in the CA's file system.
Sample value	D:\Certlog
Defined at	CA Installation Wizard
Stored at	Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration \DBLogDirectory**
Impacts	The CA must be able to obtain the appropriate path name from the registry when the CA starts.

Shared Folder

Description	Defines where the CA's transaction log files are located in the root CA's file system.
Sample value	\\{Localhost}\CertConfig
Defined at	CA Installation Wizard
Stored at	Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration**

	\ConfigurationDirectory
Impacts	Clients that cannot receive the CA certificate through group policies and need to manually import the certificate.

Distinguished Name Suffix

Description	The name maps to the name space that is used by the domain to which the CA belongs. Because the intermediate CA is configured as a stand-alone CA, the distinguished name should be mapped to the same name space that will be used for the enterprise CA.
Sample value	Domain ControllerDC=concorp,DC=contoso,DC=com
Defined at	CA configuration that occurs after the installation procedure
Stored at	Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration** *CAName***DSConfigDN**
Impacts	The distinguished name becomes part of the certificate issuer name and is also part of the CRL and AIA if replacement tokens are used. It is also used by several variables that are used to set the CRL and AIA.

CRL Distribution Point

Description	Defines the URLs where the client can locate the certificate revocation list (CRL) that is related to the certificate.
Sample value	http://www.contoso.com/pki/%3%8%9.crl ldap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10
Defined at	CA MMC
Stored at	In Windows 2000: Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Policy \FileRevocationCRLURL** Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Policy \LDAPRevocationCRLURL** Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Policy \RevocationCRLURL** In Windows Server 2003: Registry: *CAName***CRLPublicationURLs**
Impacts	Any user, computer, service, or program that verifies the root certificate

Authority Information Access (AIA)

Description	Defines the URLs where the client can locate the certificate's issuer certificate. Because a root CA issues the CA certificate to itself, no issuer needs to be specified.
Sample value	http://www.contoso.com/pki/%1_%3%4.crt ldap:///CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11
Defined at	Certification Authority MMC
Stored at	In Windows 2000: Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Policy \FileIssuerCertURL** Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Policy \LDAPFileIssuerCertURL** Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Policy \IssuerCertURL** In Windows Server 2003: Registry: *CAName***CACertPublicationURLs**
Impacts	Any user, computer, service, or program that verifies the root certificate

CRL Publication Interval

Description	Also controls also the CRL validity time
Sample value	180 days
Defined at	Certification Authority MMC
Stored at	Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration*CAName*\CRLperiod** Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration*CAName*\CRLperiodUnits**
Impacts	CA CRL publication algorithm and any user, computer, service, or program that verifies the CRL.

Delta CRL Publication Interval

Description	Defines similar to the CRL publication interval and the publication interval of the delta CRL. For an offline CA, it is recommended that you disable delta CRL publication.
Sample value	0 (which is equal to disabled delta CRL publication)
Defined at	Certification Authority MMC
Stored at	In Windows 2000: Not available. Windows Server 2003 Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration*CAName*\CRLDeltaPeriod** Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration*CAName*\CRLDeltaPeriodUnits**
Impacts	Any client that can verify the certificate validity through delta CRLs

Validity Period

Description	Defines the period of time that a certificate that was issued by the CA is valid. The validity period cannot extend the certificate validity beyond the certificate of the issuing CA.
Sample value	2 years
Defined at	Certification Authority MMC
Stored at	Windows 2000 and Windows Server 2003 Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration*CAName*\ValidityPeriodUnits** Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration*CAName*\ValidityPeriod**
Impacts	The validity time of any certificate that will be issued from that stand-alone CA.

Issuing CA Configuration Parameters

CSP (CA Certificate)

Description	The CSP is responsible for generating the certificate's key material and certificate generation.
Sample value	Microsoft Strong Cryptographic Provider
Defined at	CA Installation Wizard
Stored at	Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration**

	*****CAName***\CSP\Provider**
Impacts	CA certificate

Hash Algorithm

Description	Defines the hash algorithm that is used for hashing and signing certificate contents.
Sample value	SHA-1
Defined at	CA Installation Wizard
Stored at	CA registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration ***CAName***\CSP\HashAlgorithm**
Impacts	CA certificate

Key Length (CA Certificate)

Description	Defines the complexity of the key material that is assigned to the CA certificate. It is recommended that the key length does not exceed 4096 bits because this is the maximum interoperable key length with most applications and PKI providers. The key length of a subordinate CA is typically shorter than the key length of its parent CA.
Sample value	2048
Defined at	CA Installation Wizard
Stored at	Certificate request and is only used temporarily
Impacts	CA key material

Common Name

Description	The common name must not exceed 64 characters in length. It is important to remember that each space in the name uses three characters in the total of the overall length because of the escape character sequence (%20).
Sample value	CorporateEntCA
Defined at	CA Installation Wizard
Stored at	Windows 2000 and Windows Server 2003: Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration ***CAName***\CommonName**
Impacts	The common name becomes part of the certificate issuer name and is also part of the CRL and AIA if replacement tokens are used. The common name is used by several variables that are used to set the CRL and AIA.

CA Database Path

Description	Defines where the CA's database is located in the CA's file system.
Sample value	D:\Certlog
Defined at	CA Installation Wizard
Stored at	Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration \DBDirectory**
Impacts	The CA must be able to obtain the appropriate path name from the registry when the CA starts.

CA Log File Path

Description	Defines where the CA's transaction log files are located in the root CA's file system.

Sample value	D:\Certlog
Defined at	CA Installation Wizard
Stored at	Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration \DBLogDirectory**
Impacts	The CA must be able to obtain the appropriate path name from the registry when the CA starts.

Shared folder

Description	Defines where the CA's transaction log files are located in the root CA's file system. The shared folder is not required for an enterprise CA.
Sample value	\\Localhost\CertConfig
Defined at	CA Installation Wizard
Stored at	User-defined location during installation
Impacts	Clients that cannot receive the CA certificate through group policies and need to manually import the certificate.

Distinguished Name Suffix

Description	The name space is automatically mapped to the Active Directory namespace. The value is predefined because of the domain membership of the CA.
Sample value	CN=Configuration,DC=concorp,DC=contoso,DC=com
Defined at	Automatically defined
Stored at	Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration *CAName*\DSConfigDN**
Impacts	The distinguished name becomes part of the certificate issuer name and is also part of the CRL and AIA if replacement tokens are used. It is also used by several variables that are used to set the CRL and AIA.

CRL Distribution Point

Description	Defines the URLs where the client can locate the certificate revocation list that is related to the certificate.
Sample value	http://www.contoso.com/pki/%3%8%9.crl ldap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10
Defined at	Certification Authority MMC
Stored at	Windows 2000: Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Policy \FileRevocationCRLURL** Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Policy \LDAPRevocationCRLURL** Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Policy \RevocationCRLURL** Windows Server 2003: Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration *CAName*\CRLPublicationURLs**
Impacts	Any user, computer, service, or program that verifies the root certificate

Authority Information Access (AIA)

Description	Defines the URLs where the client can find the certificate's issuer certificate.
Sample	http://www.contoso.com/pki/%1_%3%4.crt

value	ldap:///CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11
Defined at	Certification Authority MMC
Stored at	In Windows 2000: Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration\Policy\FileIssuerCertURL** Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration\Policy\LDAPFileIssuerCertURL** Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration\Policy\IssuerCertURL** In Windows Server 2003: Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration***CAName***\CACertPublicationURLs**
Impacts	Any user, computer, service, or program that verifies the root certificate

CRL Publication Interval

Description	Also controls the CRL validity time
Sample value	7 days
Defined at	Certification Authority MMC
Stored at	Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration***CAName***\CRLPeriod** Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration***CAName***\CRLPeriodUnits**
Impacts	CA CRL publication algorithm and any user, computer, service, or computer that verifies the CRL.

Delta CRL publication interval

Description	Defines similar to the CRL publication interval and the publication interval of the delta CRL. For an offline CA, it is recommended that you disable delta CRL publication.
Sample value	1 day
Defined at	Certification Authority MMC
Stored at	Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration***CAName***\CRLDeltaPeriod** Registry: **HKLM\System\CurrentControlSet\Services\CertSvc\Configuration***CAName***\CRLDeltaPeriodUnits**
Impacts	Any client that can verify the certificate validity through delta CRLs

Appendix C: Additional Information

For additional information, see the following articles.

Q293781 Trusted Root Certificates That Are Required By Windows 2000 on the Microsoft Knowledge Base

Q293819 How to Remove a Root Certificate from the Trusted Root Store on the Microsoft Knowledge Base

Windows XP Home Page on the Microsoft Web site

PKI Enhancements in Windows XP Professional and Windows Server 2003 on the Microsoft Web site.

Windows XP Technical Resources on the Microsoft Web site

RFC 2797: Certificate Management Messages over CMS on the Internet Engineering Task Force Web site

White Paper: "Troubleshooting Certificate Status and Revocation" on the Microsoft TechNet Web site

White Paper: "Planning and Implementing Cross-Certification and Qualified Subordination Using Windows Server 2003" on the Microsoft TechNet Web site

White Paper: "Implementing and Administering Certificate Templates in Windows Server 2003" on the Microsoft TechNet Web site

White Paper: "Key Archival and Management in Windows Server 2003" on the Microsoft Web site

White Paper: "Windows Server 2003 PKI Operations Guide" on the Microsoft TechNet Web site

Certificate Autoenrollment in Windows Server 2003 on the Microsoft TechNet Web site

---

Send feedback to Microsoft