

Chapter 9

Certificate Validation

Certificate validation ensures that the certificate's information is authentic, that the certificate can be used only for its intended purposes, and that the certificate is trusted.

If certificate revocation list (CRL) checking is enabled in an application, the Microsoft Windows operating system automatically performs certificate validation and repeats the validation for each certificate in a certificate chain until it reaches the root certification authority (CA). The certificate chaining engine within the Windows operating system performs the validation testing.



More Info For more information on CRL checking and certificate validation, see the “Troubleshooting Certificate Status and Revocation” white paper listed in the “Additional Information” section of this chapter.

Certificate Validation Process

When a certificate is presented to an application, the application must use the certificate chaining engine to determine the certificate's validity. The certificate chain must be successfully validated before the application can trust the certificate and the identity represented by the certificate to encrypt data or verify a digital signature. Three distinct but interrelated processes are used to determine a certificate's validity.

- **Certificate discovery.** To build certificate chains, the certificate chaining engine must collect the issuing CA certificate and all CA certificates up to the root CA certificate. CA certificates are collected from the CryptoAPI cache, Group Policy, or Enterprise Policy, or, as a last resort, downloaded from Authority Information Access (AIA) URLs in issued certificates. Once a certificate is downloaded from a location other than the CryptoAPI cache, it is added to the user's CryptoAPI cache for faster retrieval.
- **Path validation.** When the certificate chaining engine validates a certificate, it does not stop at the presented certificate. Each certificate in the certificate chain must be validated until a self-signed root certificate is reached. Validation tests can include verifying Authenticode signatures, determining whether the

issuing CA certificate is included in the NTAAuth store, or checking for specific application or certificate policy object identifiers (OIDs). If one certificate fails a validity test, it is possible that the entire chain will be deemed invalid and not used by the calling application.

- **Revocation checking.** Once the certificate chain is built, the certificate chaining engine checks the revocation status of each certificate in the chain. When running Windows XP or Windows Server 2003, the chaining engine checks revocation as the chain is built. By contrast, Windows 2000 and earlier operating systems do not perform revocation checking until the chain is assembled.

Certificate Validity Checks

When a certificate is presented to an application, the certificate chaining engine tests the following components:

- **Certificate contents.** A certificate must have information in all required X.509 standard fields. If a required field is missing or populated incorrectly, the certificate is considered invalid.



Note The certificate chaining engine excludes all invalid certificates found during the certificate discovery process. Invalid certificates are used by the certificate chaining engine when building certificate chains.

- **Certificate format.** A certificate must conform to a valid X.509 standard for digital certificates. The certificate chaining engine rejects a certificate that does not follow X.509 version 1, version 2, or version 3 formats.
- **Critical extensions.** If the certificate contains any X.09 version 3 certificate extensions that are marked as critical, the chaining engine will identify the critical extensions to the calling application. If the calling application does not understand the critical extension, the application will consider the certificate to be invalid.
- **Policy validation.** If the application that calls the certificate chaining engine expects a specific application policy or certificate OIDs in the certificate, and the required policy or OIDs are not contained within the certificates in the CA chain, the certificate chaining engine considers the certificate to be invalid.
- **Revocation check.** The certificate chaining engine calls any installed revocation providers to ensure that the certificate's serial number is not in the issuing CA's CRL. If the certificate is in the CRL listing, the certificate is considered to be invalid. This revocation check is performed for each certificate in the certificate chain below the root CA certificate.

- **Root check.** The certificate chain assembled by the certificate chaining engine must chain to a trusted root CA or be included in a certificate trust list (CTL) manually configured by the organization or downloaded from Windows Update. If the chain terminates at a nontrusted root CA or does not chain to a self-signed root CA certificate, the presented certificate is considered to be invalid.
- **Signature check.** When a CA issues a certificate, the CA's private key digitally signs the issued certificate's contents. If the contents are modified or corrupted, the digital signature validation fails, resulting in an invalid certificate.
- **Time validity.** The current date and time must fall within the presented certificate's validity period. If it doesn't, the certificate chaining engine considers the certificate to be invalid.

Certificate Revocation

Certificate revocation is necessary when you must terminate a certificate's usage before the validity period expires. When a certificate is revoked, a certificate manager must select the certificate to revoke in the Certification Authority console and provide a reason for revocation. The serial number of the certificate is then stored in the CA's database with a reason code specifying why the certificate was revoked; it can then be used to publish a CRL, etc.

Types of CRLs

The Windows Server 2003 public key infrastructure (PKI) supports two different but related types of CRLs: base CRLs and delta CRLs.

A *base CRL* contains the serial numbers of certificates revoked by the CA that are signed with the CA's private key. If you renew a CA's certificate with a new key pair, the Windows Server 2003 CA maintains two separate CRLs—one for each key pair maintained by the CA. Base CRLs are recognized by all versions of the Windows operating system.

A *delta CRL* contains only the serial numbers of certificates revoked by the CA since the last base CRL publication. Again, if the CA's certificate is renewed with a new key pair, separate delta CRLs are maintained for each CA key pair. Delta CRLs allow you to publish revocation information more quickly and allow smaller updates to be downloaded by client computers.



Caution Delta CRLs are only supported by Windows XP and Windows Server 2003 operating systems. Older operating systems will ignore the delta CRL and determine revocation information by inspecting the base CRL. Support for delta CRLs is expected in the Windows 2000 Service Pack 5.

CRL Retrieval Process

When a client computer checks the revocation status of a certificate, it first checks for the desired base CRL or delta CRL in the CryptoAPI cache. If the base CRL or delta CRL is found, the CRL is checked to determine whether the CRL is time-valid. Like certificates, a CRL has a validity period defined by the CRL publication interval. If a time-valid CRL is found in the CryptoAPI cache, that version of the CRL is used for revocation checking, even if an updated version has been published manually. The cached CRL is used to prevent excess network traffic. Use of a cached CRL also follows the recommendations in RFC 3280 to acquire an updated CRL only when the previous CRL expires.



Warning Microsoft does not support designs that manually delete the cached version of a CRL from the CryptoAPI cache.



More Info The process described here follows the definition of CRL usage in RFC 3280, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,” listed in the “Additional Information” section of this chapter.

Revocation Reasons

The following revocation reasons are available for CRLs:

- **AffiliationChanged.** An individual is terminated, resigns, or dies. This revocation reason also can be used if a person changes roles within an organization and no longer requires use of the certificate associated with the previous role.
- **CACompromise.** You suspect that a CA’s private key is compromised and in the possession of an unauthorized individual. If a CA’s private key is revoked, all certificates below that CA in the CA hierarchy are considered revoked.
- **CertificateHold.** A temporary revocation that indicates a CA will not validate a certificate at that specific time.



Tip Although CertificateHold allows a certificate to be unrevoked, use of the CertificateHold reason code is not recommended, as it becomes difficult to determine whether a certificate was valid at a specific time.

- **CessationOfOperation.** A CA is decommissioned and all certificates issued by the CA are no longer in use.



Tip You cannot decommission a CA if any of the certificates issued by the CA are in use. Even if you do not plan to issue any additional certificates, the CA must still publish CRL information at regular intervals for revocation checking purposes.

- **KeyCompromise.** You suspect that the private key associated with a certificate is compromised. For example, if a laptop belonging to a user in your organization is stolen, it is possible that any private keys stored on the laptop are compromised.
- **RemoveFromCRL.** Unrevokes a certificate revoked using `CertificateHold`. The unrevoking process still lists the certificate in the CRL, but the certificate also appears in a delta CRL with the revocation code set to `RemoveFromCRL`. When the next base CRL is published, the CA removes the certificate from all forms of the CRL.
- **Superseded.** A new certificate must be issued if a user's certificate is replaced for any reason with a new updated certificate. For example, if you update a certificate template and reissue certificates, you can revoke the previous certificate with this reason code.
- **Unspecified.** You can revoke a certificate without providing a specific revocation code. Using `Unspecified` is not recommended, however, as it does not provide an audit trail identifying why a certificate was revoked.

Revoking a Certificate

To revoke a certificate, a user must be designated as a certificate manager by assigning the user or a group the user is a member of the Issue and Manage Certificates permission at the issuing CA. The permission assignment is performed by a CA Administrator or a user assigned the Manage CA permissions. You can use the following process to verify the permission assignment:

1. Log on to the CA computer.
2. From Administrative Tools, open the Certification Authority console.
3. In the console tree, right-click *CAName* (where *CAName* is the logical name of the CA) and click Properties.
4. In the *CAName* Properties dialog box, select the Security tab to ensure that the user account or a group that the user is a member of is assigned the Issue and Manage Certificates permission.



Note If you want to assign a new user or security group the certificate manager role to allow them to revoke certificates, assign the user or security group the Issue and Manage Certificates permission.

Once you assign the necessary permissions, the following procedure revokes a certificate:

1. From Administrative Tools, open the Certification Authority console.
2. In the console tree, expand *CAName* and click Issued Certificates.
3. In the details pane, find the certificate that you need to revoke, right-click the certificate, point to All Tasks, and click Revoke Certificate.
4. In the Certificate Revocation dialog box, in the Reason Code drop-down list, select the appropriate reason code and click Yes.

Building Certificate Chains

The certificate chaining engine builds chains by inspecting specific extensions in a presented certificate. There are different processes the certificate chaining engine uses to determine the issuing CA's correct certificate. The actual selection is based on the current certificate's attributes. Specifically, the certificate chaining engine examines a combination of the following certificate fields and X.509 version 3 certificate extensions:

- **Authority Key Identifier (AKI) extension.** The matching method the certificate chaining engine performs is based on the contents of the AKI extension. When using the Windows Server 2003 PKI, the AKI extension can contain:
 - The subject and serial number of the issuing CA's certificate.
 - The hash of the issuing CA's public key.
 - Nothing, or is not present in the evaluated certificate.
- **The Issuer field.** If an AKI extension is not present, the certificate chaining engine determines the issuing CA's name from the evaluated certificate's Issuer field.

- **The Subject of the issuing CA certificate.** The subject is used to identify the issuing CA certificate. If the AKI contains the subject and the serial number of the issuing CA certificate, the CA certificate with the same serial number and subject is selected.
- **The Serial Number field of the issuing CA certificate.** If the AKI contains the subject and the serial number of the issuing CA certificate, the CA certificate with the same serial number and subject is selected.
- **The Subject Key Identifier (SKI) extension of the issuing CA certificate.** If the AKI contains the hash of the issuing CA's public key, the CA certificate's SKI contains a matching hash value.

These fields and extensions are used by the certificate chaining engine to build certificate chains. Based on the contents of the evaluated certificate's AIA extension, the chaining engine builds the certificate chain using an exact match, key match, or name match.

Exact Match

In the event that an evaluated certificate contains the issuing CA's subject name and serial number, the certificate chaining engine uses an exact match (also known as a key and name match), to find the issuing CA's certificate. The chaining engine searches for a CA certificate with the subject name and the serial number defined in the evaluated certificate's AKI extension. (See Figure 9-1.)

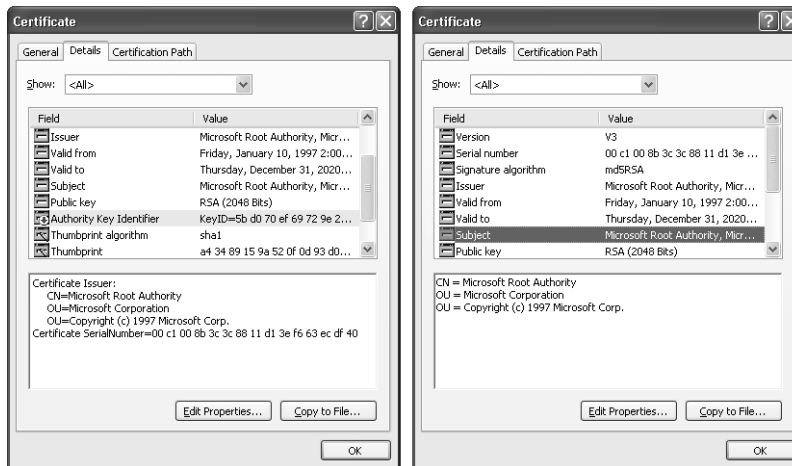


Figure 9-1 An exact match

The left certificate's AKI extension contains the subject and serial number of the issuing CA's certificate. Note that the certificate on the right has a matching serial number and subject name.



Note A single match can happen only in the case of an exact match. Anytime you renew a CA's certificate, the new certificate has a different serial number.

Key Match

If an evaluated certificate's AKI extension contains only the hash of the issuing CA's public key, the certificate chaining engine searches for CA certificates that have a matching value in each CA certificate's SKI extension. (See Figure 9-2.)

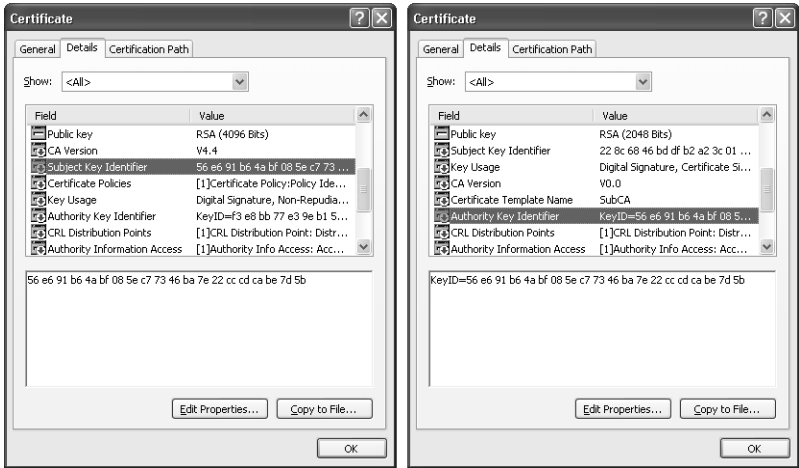


Figure 9-2 A key match

In the certificate on the right, the AKI extension contains the hash of the issuing CA's public key. In the issuing CA certificate on the left, the same public key hash exists in the SKI extension. For the match to be successful, the two hashes must be calculated using the same hash algorithm. Even if the issuing CA certificate does not have an SKI extension, a key match is still possible if the hash algorithm used to calculate the hash of the public key is SHA-1, the default hash algorithm used by the Microsoft CA and CryptoAPI. If other hash algorithms are used, the resulting hash of the public key must exist in both the evaluated certificate's AKI extension and the CA certificate's SKI extension.



Note There can be multiple matches when key matching is used to build a certificate chain. This scenario, known as ambiguous chaining, occurs when the CA certificate is renewed with the same key pair. Both versions of the CA certificate contain the same value in the SKI extension.

Name Match

If no information exists in the AKI, or if the AKI does not exist in the evaluated certificate, the certificate chaining engine uses a name match to find the issuing CA's certificate. To perform name matching, the certificate chaining engine matches the contents of the evaluated certificate's Issuer field to the Subject field of the issuing CA's certificate. (See Figure 9-3.)



Note The name matching process is case sensitive.

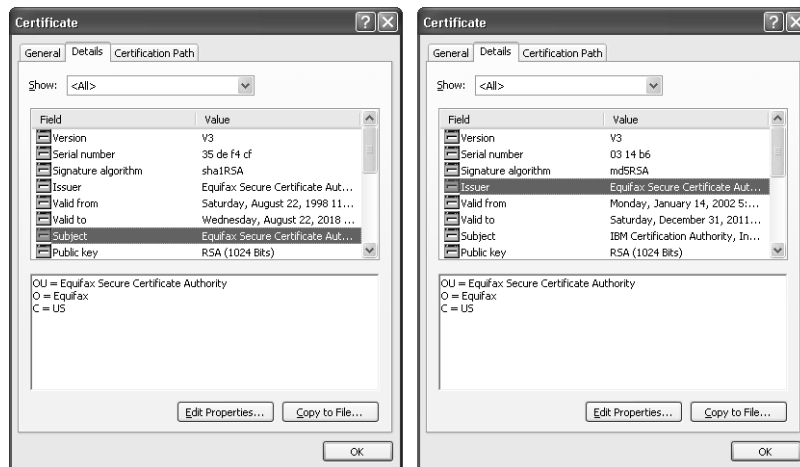


Figure 9-3 A name match

The right certificate's Issuer field contains the same subject name as the left certificate's Subject field.



Note Multiple matches are possible when name matching is used to build a certificate chain. This scenario occurs when the CA certificate is renewed with either the same key pair or a new key pair. When the CA certificate is renewed, the Subject of the CA certificate does not change.

Designing PKI Object Publication

To enable certificate validation, you must ensure that a CA's certificate and CRL are available for download by the certificate chaining engine. This is done by confirming that the certificate and CRL are available by using the desired protocols from the desired locations and are published at the required intervals.

Choosing Publication Protocols

Determining the protocols used for CA certificate and CRL retrieval is the first step in choosing publication points. The following protocols are available with Windows Server 2003 PKI:

- **HTTP.** The Hypertext Transfer Protocol (HTTP) provides the most flexibility. Almost all client computers have a Web browser installed that allows access to HTTP URLs. The HTTP protocol is also useful when computers that are not members of the forest require access to the CA certificate or CRL. The CA certificate and CRL also can be published to a Web cluster to provide redundancy and high availability.



Note There should be no need to implement Secure Sockets Layer (SSL) protection for the Web server hosting the CA certificate or CRL publication points. The CA certificates and CRLs are digitally signed objects that do not require transport level security to provide data integrity. In addition, the use of SSL can cause recursion of revocation checks. To download the updated version of the CRL, you must check the CRL to ensure that the certificate that signed the CRL is valid.

- **LDAP.** The Lightweight Directory Access Protocol (LDAP) provides high availability by publishing the CA certificate and CRL to the Microsoft Active Directory Configuration naming context. LDAP URLs can be accessed by any forest members that can resolve them. This includes Windows 2000 and later and Windows 98, Windows Me, and Windows NT 4.0 computers with the Directory Services Client installed.



Note If an explicit X.500 distinguished name is used in the LDAP URL, Active Directory must contain an explicit referral to the object.



Note LDAP URLs can be accessed by operating systems other than Windows if the LDAP URL is modified to include the DNS name of the LDAP server in the LDAP URL. For example, rather than publishing the CDP URL as LDAP:///CN=CAName,CN=CAComputer,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,*ForestRootDomain*, you would publish the CDP URL as LDAP://*Webserver*/CN=CAName,CN=CAComputer,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,*ForestRootDomain*. In addition, if published in Active Directory, the permissions of the CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,*ForestRootDomain* container must be modified to allow anonymous access.

- **FTP.** The File Transfer Protocol (FTP) provides access to FTP clients for the download of CA certificates and CRLs. Although not typically used, FTP URLs are supported by Microsoft clients with the TCP/IP protocol stack.
- **File.** The file protocol provides access to file shares using the Common Internet File System (CIFS) or Server Message Blocks (SMBs). Although not commonly used for CA certificate and CRL retrieval, the file protocol is sometimes used to publish CA certificates and CRLs to remote file locations.

You can implement more than one publication protocol. When you define the publication points, the order in which they appear on the CA's Extensions tab is the order in which the client computers search the URLs.

Choosing Publication Points

Once you choose the publication protocols, you must choose *where* to publish the CA certificates and CRLs. The location decision includes the physical servers where you publish the files and the servers on the corporate network: intranet or extranet.

Choose publication points according to the following rules:

- If most computers are running Windows 2000 or later and are members of the forest, you should include an LDAP URL that references the Active Directory Configuration naming context. This location is published to all domain controllers in the forest and ensures availability and fault tolerance.

- If you have several nonforest computers or third-party operating systems, such as UNIX, you should include Web server publication points for HTTP URLs.
- If certificates are to be evaluated from the external network, the CA certificate and CDP must be published to an externally accessible location, such as a Web server or LDAP server in the demilitarized zone (DMZ) of the network.
- File publication points typically are not used for CA certificate and CRL retrieval. File publication points are more common for publishing CA certificate and CRL information to remote servers.
- The URL order is determined by the type of network clients. The order should be set so that the majority of clients can retrieve the CA certificate or CRL from the first URL in the listing. If a client cannot retrieve the CA certificate or CRL from the first URL, the client times out in an attempt to connect, and then proceeds through the next URLs in the listing.



Note The URL order is not important to all operating systems. Some UNIX systems use their own methods to determine what order URLs are fetched when multiple URLs exist in the CDP extension.

- Delta CRLs are published more frequently than base CRLs. You can consider not publishing delta CRLs to LDAP locations because of Active Directory replication latency. Instead, publish delta CRLs to HTTP locations. The Active Directory replication interval must be more frequent than the delta CRL validity period.

URL Ordering Issues

When you implement multiple URLs in a CDP extension, the order of the URLs is important. If you do not choose the correct order, a client will spend a specific amount of time attempting to connect to each URL in the listing before attempting to use the next URL in the listing. The default behavior for a Windows client is:

- The maximum timeout for all CRL retrievals is 20 seconds. If a download did start, it will continue after the 20-second interval, perhaps resulting in a success the next time a connection is attempted.

- The first CDP location is given a maximum of 10 seconds to succeed. If the CRL cannot be downloaded in the 10-second interval, the certificate chaining engine will proceed to the next URL in the listing. You should ensure that the first URL listed can be accessed by the greatest number of computers. For example, if several computers are not members of the forest, or use another operating system, such as UNIX, consider moving the default first entry of `LDAP:///CN=CAName,CN=CAComputer,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=ForestRootDomain` to a lower placement in the URL listing.
- Subsequent CDP locations will each use a maximum of one-half of the remaining time to retrieve a specific CRL object before continuing to the next location.
- Each location download is attempted in sequential order. If CryptoAPI is unable to retrieve a CRL for any reason during the allotted maximum timeout interval, such as invalid path, access denied, etc., an error of “revocation offline” will be returned to the application.

Careful planning of the publication locations will prevent timeout errors from affecting certificate revocation status checking.

Choosing Publication Intervals

When you configure a CA, one of the design decisions is how frequently to publish the base CRL and the delta CRL. Before discussing these decision points, it is useful to review the interaction of base and delta CRLs. (See Figure 9-4.)

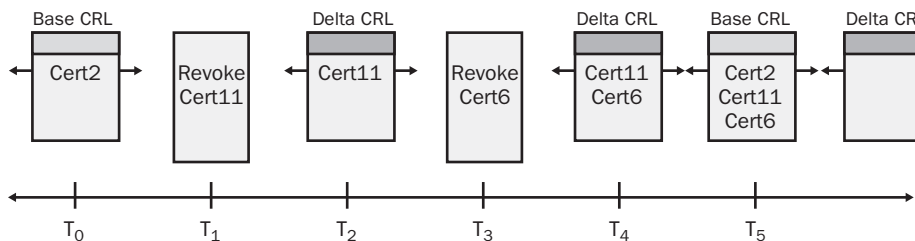


Figure 9-4 Base and delta CRL publication

1. In Figure 9-4, the initial base CRL is published at time T_0 and includes one revoked certificate, Cert2.
2. At time T_1 , Cert11 is revoked with a revocation reason of `AffiliationChanged`.

3. At time T2, when the delta CRL is published, the delta CRL contains only one entry, Cert11.
4. At time T3, Cert6 is revoked with a revocation reason of Superseded.
5. At time T4, when the next version of the delta CRL is published, the delta CRL contains both Cert6 and Cert11.
6. At time T5, when the next version of the base CRL is published, the base CRL contains three certificates: Cert2, Cert6, and Cert11. In addition, an empty delta CRL is published with no entries in the delta CRL.

Publication intervals should be based on the answers to the following questions:

- **What is the maximum period your organization is willing to accept a revoked certificate as valid?** If you use the default publication intervals, the base CRL is published weekly and the delta CRL is published daily. You must redefine these publication intervals to meet your organization's acceptable risk level.
- **What operating systems run on your organization's network?** If your client computers run Windows 2000 or earlier versions, you must define shorter CRL publication intervals so that computers have up-to-date information. Only Windows XP and Windows Server 2003 operating systems support delta CRLs. If you run another operating system, such as UNIX, you must verify whether this operating system supports delta CRLs.



Note Windows 2000 Service Pack 5 is expected to add delta CRL recognition to all Windows 2000 client computers.

- **What is the network traffic associated with CRL retrieval?** The more frequently you publish the base CRL, the more often clients download the base CRL, which increases the network traffic associated with CRL retrieval.
- **How large is the delta CRL?** Publishing several delta CRLs between each base CRL publication can result in a larger delta CRL. The goal of a delta CRL is to reduce the size of downloaded CRLs, in addition to making more frequent updates. In the case of a larger delta CRL, consider reducing the publication interval for base CRLs or publishing delta CRLs less frequently.
- **How often are certificates revoked?** The number of certificates revoked within a period greatly influences the publication interval for both base and delta CRLs. You must define publication intervals so that revoked certificates are recognized as soon as possible. You must balance the interval against the network load resulting from CRL-download traffic.

- **What is the Active Directory replication latency on your network?** The delta CRL and base CRL publication intervals are limited by the replication latency of Active Directory. Because the replication latency can be eight hours or longer in some cases, defining CRL publication to an interval of less than eight hours can result in the CRL being unavailable until Active Directory replication is completed. Replication latency results in the failure of the path-validation process due to the inability to download an updated CRL.
- **What is the expected time to recover from a disaster?** If Certificate Services fails, you must rebuild the CA and restore the CA database and registry settings before the previous CRL expires. If the CRL publication interval is shorter than the amount of time required to recover a failed CA, certificates issued by the CA will fail revocation checking due to the inability to download an updated CRL.

Troubleshooting Publication Points

The misconfiguration of CA certificate and CRL publication points is the most common error in a PKI. If the publication points are referenced incorrectly, certificate validation errors, CA failures, issuance failures, logon failures, and so on can result.



Note If the certificate chaining engine cannot find an updated CRL as referenced in the CDP extension of a certificate, the chaining engine invalidates the certificate with a revocation status: “Cannot determine the revocation status of the certificate.” Most applications consider this revocation status (also known as the revocation unknown status code) to be the equivalent of a revoked certificate when strong CRL checking is enabled because it is safer to reject the certificate than to accept a revoked certificate.

To prevent publication errors from occurring on your network, you should use tools to ensure that the publication points are configured correctly. The following tools are available for validating the AIA and CDP URLs:

- Certutil
- PKI Health Tool
- CryptoAPI Monitor (CAPIMON)

Certutil

Certutil.exe, a utility in the Windows Server 2003 Administration Pack (adminpak.msi), allows a PKI administrator to manage a PKI from the command line. One of the abilities of certutil.exe is to verify certificate chaining and CRL retrieval. By using the command `certutil -verify -urlfetch CertificateFileName`, you can verify the ability to retrieve CA certificates and CRLs for the entire certificate chain of the *CertificateFileName* file.

For example, if you were to verify the certificate `brian.cer` by typing **certutil -verify -urlfetch brian.cer**, the output would fetch each CDP and AIA URL in the certificate and report on the status of the URL. A validated LDAP URL for a base CRL appears like this:

```
Verified "Base CRL (36)" Time: 0
[1.0] ldap:///CN=Fabrikam%20Issuing%20CA,CN=IssuingCA,
CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,
DC=fabrikam,DC=com?certificateRevocationList?base?objectClass=
cRLDistributionPoint
```

Likewise, a validated HTTP URL for a base CRL appears like this:

```
Verified "Base CRL (36)" Time: 0
[0.0] http://www.fabrikam.com/CertData/Fabrikam%20Issuing%20CA.crl
```

The output reports on every URL in every certificate in the certificate chain, from the examined certificate to the certificate chain's root CA. If certutil is unable to connect to one of the referenced URLs, the output indicates the following:

```
Failed "CDP" Time: 0
Error retrieving URL: Error 0x800701f6 (WIN32: 502)
http://www.fabrikam.com/CertEnroll/Fabrikam%20Issuing%20CA.crl
```

If any errors are encountered by certutil, the final lines of the output reports that revocation checking failed, as shown here:

```
ERROR: Verifying leaf certificate revocation status returned. The revocation
function was unable to check revocation because the revocation server was offline.
0x80092013 (-2146885613)
CertUtil: The revocation function was unable to check revocation because the
revocation server was offline.
```

PKI Health Tool

The Windows Server 2003 Resource Kit includes the PKI Health Tool (pkiview.msc), a retrieval tool for URLs in both the CDP and AIA extensions of all certificates in the certificate chain. The PKI Health Tool reports on the status of each URL configured in the CA hierarchy using status codes of OK, Expired, and Unable to download.

To use the PKI Health Tool, you must initialize the associated dynamic link library (DLL) with the following procedure:

1. Open a command prompt.
2. In the command prompt, type **regsvr32 pkiview.dll** and press ENTER.
3. In the Regsvr32 dialog box, click OK.



Note If you install the Windows Server 2003 Resource Kit Tools, the PKI Health Tool and associated pkiview.dll files are automatically installed and registered. Use this procedure if you only want to install the PKI Health Tool, not the entire resource kit.

Once the DLL is registered, you can open the PKI Health Tool by running `pkiview.msc`. (See Figure 9-5.)

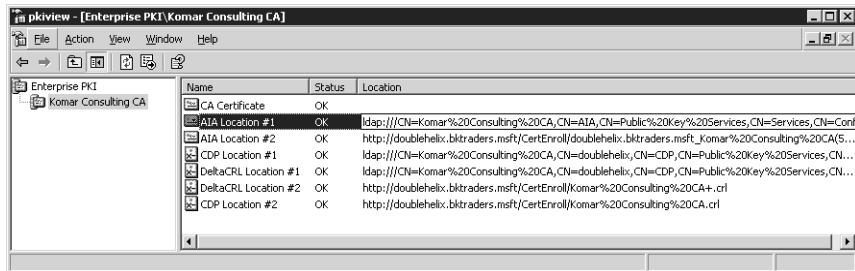


Figure 9-5 The PKI Health Tool console

Within the PKI Health Tool console, you can view the status for each AIA and CDP URL. The status codes will include:

- **OK.** The CA certificate or CRL at the referenced URL is valid.
- **Expiring.** The CA certificate or CRL at the referenced URL is near expiration.



Note You can define the expiration interval for CA certificates, CRLs, and delta CRLs within the PKI Health Tool to match the publication intervals used by your organization. For example, if you publish base CRLs every day, you could define the expiration warning interval to be eight hours before expiration rather than the default of two days.

- **Expired.** The CA certificate or CRL at the referenced URL is expired.
- **Unable to download.** The CA certificate or CRL could not be downloaded from the referenced URL.

Case Study: Choosing Publication Points

This case study will test your knowledge of choosing CRL and CA certificate publication points.

Design Requirements

You are responsible for defining the CA certificate and CRL publication points for your CA hierarchy. Your organization, Northwind Traders, is implementing a three-tier CA hierarchy, as shown in Figure 9-6.

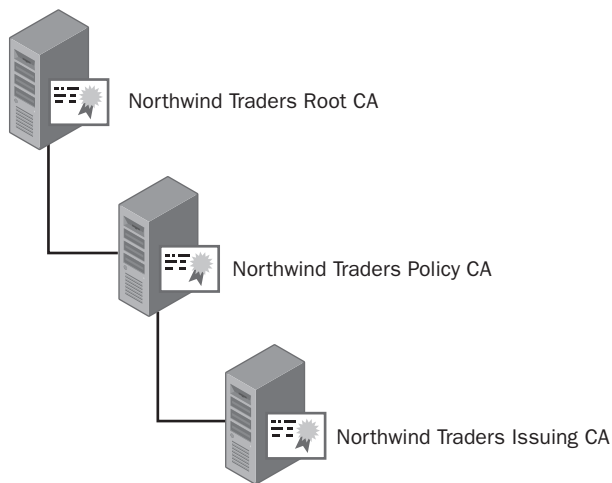


Figure 9-6 The Northwind Traders CA hierarchy

The following requirements for your network should influence your decision on where to publish the CA certificate and CRLs for your CA hierarchy:

- Northwind Traders implements an Active Directory forest with a single domain named corp.nwtraders.com on the production network.
- Externally accessible Windows 2000 Web servers are located in a DMZ and are not members of the corp.nwtraders.com domain.
- The client computers run Windows 2000 Professional and Windows XP Professional.
- Some Web servers run BSD UNIX with Apache Web servers.
- All access to Web servers is authenticated by using certificate-based authentication.
- The Northwind Traders security policy requires that all applications implement strong CRL checking.

Case Study Questions

1. What URLs do you include in the Northwind Traders root CA certificate for the AIA and CDP extensions?
2. Are there any network design issues that prevent you from implementing an LDAP URL as the first URL in the list of available URLs for CA certificates and CRLs?
3. What form of URL should you implement as the first URL in CDP and AIA URL listings?
4. What protocol by default provides redundancy and high availability in an Active Directory environment?
5. How do you provide redundancy and high availability for HTTP URLs?

Additional Information

- “Troubleshooting Certificate Status and Revocation” (www.microsoft.com/technet/security/topics/crypto/tshtcrl.msp)
- RFC 3280, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” (www.ietf.org/rfc/rfc3280.txt)
- CAPIMON tool (www.microsoft.com/downloads/details.aspx?FamilyID=0bfe87a8-4e79-4441-9d4c-0cab35d49a01&DisplayLang=en)
- Knowledge Base Article 320528, “How to Configure Active Directory to Allow Anonymous Queries” (Windows 2000)
- Knowledge Base Article 326690, “Anonymous LDAP Operations to Active Directory Are Disabled on Windows Server 2003 Domain Controllers”



Note Microsoft Knowledge Base articles can be found at <http://support.microsoft.com>. Enter the article number in the Search the Knowledge Base text box.

