Windows 2000 Server

Chapter 12 - Planning Your Public Key Infrastructure

Microsoft® Windows® 2000 supports a comprehensive public key infrastructure (PKI). A PKI is a system of digital certificates, certification authorities, and other registration authorities that verify and authenticate the validity of each party involved in an electronic transaction through the use of public key cryptography.

You can design a PKI that meets your public key security needs using Microsoft® Certificate Services or other certificate services.

In This Chapter

Chapter Goals

This chapter will help you to develop the following planning documents:

- Public key certificate requirements
- Policies for how certificates will be issued and used
- Certification authority trust hierarchy design
- Certificate life cycle policies and processes
- Policies governing certificate revocation
- Strategies for certificate backup and disaster recovery
- Timetable for PKI deployment and rollout

Related Information in the Resource Kit

- For more information about the basic concepts of cryptography-based security, PKI, and public key technology, see "Cryptography for Network and Information Security" in the *Microsoft® Windows® 2000 Server Resource Kit Distributed Systems Guide.*
- For more information about security solutions using public key technology, see "Choosing Security Solutions That Use Public Key Technology" in the *Microsoft Windows 2000 Server Resource Kit Distributed Systems Guide.*

Overview of Public Key Infrastructure

Public key infrastructure (PKI) is an underlying technology of Windows 2000 that enables a variety of features relating to authentication and encryption. Therefore, your plans for PKI need to be defined early in the deployment process.

This section presents a brief overview of the PKI features and tools in Windows 2000.

How PKI Works

A PKI is based on *certificates*. A certificate is a digitally signed statement containing a public key and the name of the subject. There can be multiple types of names in the certificate by which the subject is known, such as a directory name, e-mail name, and Domain Name Service (DNS) name. By signing the certificate, the certification authority verifies that the private key associated with the public key in the certificate is in the possession of the subject named in the certificate.

A certification authority, frequently a third-party company, issues a trusted user a certificate containing a public key. This certificate can be freely distributed. The public key can be used to encrypt data that can only be decrypted using an associated private key, which is also provided to the user. The user keeps the private key secure, so that no one else has access to it. The private key can be used to create a digital signature that can be confirmed by the public key.

The basic idea of public key cryptography is that there are two keys that are related. One key can be passed openly and freely between parties or published in a public repository; the other key must remain private. There are also different types of public key algorithms, each with its own characteristics. This means that it is not always possible to substitute one algorithm for another. If two algorithms can perform the same function, the detailed mechanism by which that result is obtained varies. With public key cryptography, the two keys are used in sequence. If the public key is used first, followed by the private key, then this is a key exchange operation. If the private key is used first, followed by the public key, this is a digital signature operation.

You can create your own certification authorities within your enterprise, and you can use third-party companies that provide commercial certification services.

PKI processes information in a way that simultaneously identifies and authenticates the source. It makes identity interception very difficult and prevents masquerading and data manipulation. Table 12.1 describes some of the ways you can use PKI in an enterprise.

Table 12.1 Leading Applications for Digital Certificates

Application	Uses
Secure e-mail	Secure e-mail clients use certificates to ensure the integrity of e-mail and to encrypt e-mail messages for confidentiality.
Secure Web communications	Web servers can authenticate clients for Web communications (using client certificates) and provide confidential, encrypted Web communications (using server certificates).
Secure Web sites	Internet Information Services (IIS) Web sites can map client certificates to authenticate users to control their rights and permissions for Web site resources.
Digital signing of software files	Code-signing tools use certificates to digitally sign software files to provide proof of file origin and to ensure the integrity of data.
Local network Smart Card authentication	The Kerberos logon protocol can use certificates and the private key stored on smart cards to authenticate network users when they log on to the network.
Remote access Smart Card authentication	Servers that are running the Routing and Remote Access service can use certificates and the private key stored on smart cards to authenticate network users when they log on to the network.
IPSec authentication	IPSec can use certificates to authenticate clients for IPSec communications.
Encrypting File System (EFS) recovery agent	Recovery agent certificates enable recovery of EFS files encrypted by other users.

Prerequisites for Implementing PKI

Implementing PKI in your enterprise is a multiple-part process requiring planning and experimentation through pilot programs. Some features of Windows 2000, such as the Encrypting File System (EFS) and IP security (IPSec), can provide their own certificates without any special preparation on the part of the network administrator. You can deploy these features immediately. Other security features might require a hierarchy of CAs. A CA hierarchy requires planning.

The first business policy decisions you make will have to do with selecting the CAs, both internal and external, that will be the source of your certificates. A typical CA hierarchy has a three-level architecture. It is recommended that you have one root CA, and that it be offline. You need a second level of CAs to implement certificate policy. This level also needs to be offline. The third level is the issuing CAs. You can have internal or external CAs at this level. Internal network authentication and data integrity can be handled by a local certifying authority, such as your IT department. Internet transactions and software signing might require third-party certificates in order to establish public credibility.

While selecting your CAs, give some thought to your cryptographic service provider (CSP). The CSP is the software or hardware that provides encryption services for your CA. If the CSP is software based, it will generate a public key and a private key, often referred to as a key pair, on your computer. If the CSP is hardware based, such as a smart card CSP, it might instruct a piece of hardware to generate the key pair.

The standard CSP for Windows environments is the Microsoft Base cryptographic service provider, which provides 40-bit key lengths. Windows 2000 supports 40/56-bit encryption and is exportable. For greatest security (and greater speed), consider using a hardware-based CSP, available from third-party vendors.

Greater security usually means greater cost, both in terms of expense for hardware and in CPU cycles devoted to encryption. Greater security is not always cost effective, but it is available when needed. For extreme levels of security, consider a hardware CSP for CAs and smart cards for users.

How to Implement PKI

Provision for public key infrastructure certificates is built into Windows 2000 and most software that supports enterprise business computing. To learn about Windows 2000 PKI features, explore the following sections.

Creating a Local Certification Authority

You can create a local CA on your Windows 2000 server. There are several types of CAs to choose from. One type is the enterprise CA, which can issue certificates for purposes such as digital signatures, encrypted e-mail, Web authentication, and Windows 2000 domain authentication through smart cards. The enterprise CA will issue certificates based on requests from users or other entities, and it requires the use of the Active Directory™ directory service.

A stand-alone CA issues certificates based on requests from users or other entities; however, unlike the enterprise CA, it does not require the use of Active Directory. Stand-alone CAs are primarily intended for use with extranets or the Internet.

CAs can also fulfill various hierarchical roles such as root CA, subordinate CA, and issuing CA. For considerations about certification hierarchies, see "Define Certificate Policies and Certification Authority Practices" later in this chapter.

To create a local CA on your Windows 2000–based server

1. Click **Start**, point to **Settings**, and then click **Control Panel**.
2. Double-click Add/Remove Programs, and click Add/Remove Windows Components.
3. Add Certificate Services, and install an enterprise root CA.

For more information about installing a local certification authority, see Windows 2000 Server Help.

After you create a local CA, you can monitor and manage it by using the Certification Authority snap-in to Microsoft Management Console (MMC).

You can also view your PKI certificates.

To view your personal set of PKI certificates

1. Open Microsoft Internet Explorer.
2. On the **Tools** menu, click **Internet Options**.
3. Click the **Content** tab of the resulting dialog box. The buttons in the center section of this tab display your current certificates, trusted certifying authorities, and trusted software publishers.

Managing Your Certificates

To manage your certificates, use the Certificates snap-in to MMC. Note that this snap-in has two display modes, the Logical Certificate Stores display and the Certificate Purpose display. Click the Certificates node (top-level node) to highlight it. On the **View** menu, click **Options**. Familiarize yourself with each of the two display modes.

To request a new certificate while in this snap-in, right-click the appropriate node in the Certificate Purpose view and, on the **All Tasks** menu, click **Request New Certificate**.

Using the Certificate Services Web Pages

When your Windows 2000 site is operational, you can allow users to request their own certificates from your internal certification authority. You must have a CA configured and running, and IIS must also be configured and running. Access the enrollment Web pages through http:// *computer_DNS_name*/certsrv/.

Setting Public Key Policies in Group Policy Objects

A number of PKI policies can be set in a Group Policy object and thereby applied to computers in domain and organizational unit scope. Open the Group Policy snap-in to MMC to the appropriate Group Policy object. The PKI entries are located under Computer Configuration:

```
Group_Policy_Object
X Computer Configuration
X Windows Settings
X Security Settings
X Public Key Policies
```

Certificate trust lists and CA root certificates are part of Group Policy objects, and contain the CAs to be trusted by recipients of the Group Policy. These are the Enterprise Trust and Trusted Root Certification Authority containers under Public Key Policies, respectively.

Building Your Public Key Infrastructure

The Windows 2000 PKI provides a framework of services, technology, and protocols based on standards that enable you to deploy and manage a strong information security system using public key technology. Windows 2000 supports a variety of public key security features required by distributed security services. For example, Windows 2000 supports public key cryptography operations required for EFS without the need to deploy additional infrastructure or CAs.

However, many security solutions (such as secure e-mail, smart card authentication, and secure Web communications) require that you design, test, and deploy additional components of the PKI, including CAs, certificate enrollment, and renewal to support these types of applications. You might also want to deploy certificate services to support EFS users and multiple recovery agents or IPSec authentication for clients not running Kerberos authentication or not able to use Kerberos authentication for establishing trust relationships (across untrusted Windows 2000 domains or with a computer that is not a member of a Window 2000 domain).

Furthermore, to meet special requirements for your organization, you might want to develop and deploy custom applications and certificate services.

Figure 12.1 shows a basic process that you can use to design, test, and deploy a PKI in your organization.

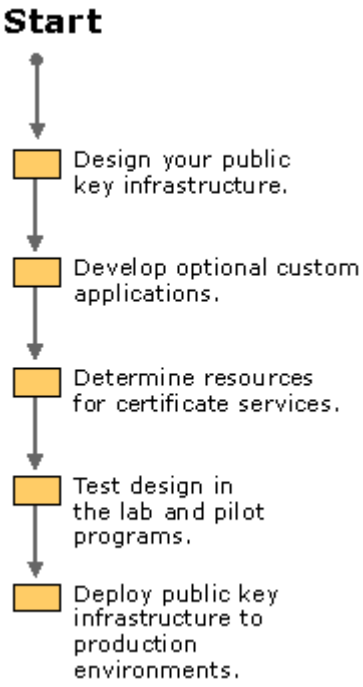

Figure 12.1 Process Flow Chart for Designing a PKI in Your Organization

You can design and deploy your PKI using Microsoft Certificate Services. You can also use Windows 2000–compliant third-party CAs to build part or all of your PKI. The basic process for building your PKI is the same whichever certificate services you use. However, the actual implementation details for building your PKI will differ depending on the specific certificate services technology. For more information about the components and features of the Windows 2000 public key infrastructure, see "Choosing Security Solutions That Use Public Key Technology" in *The Microsoft Windows 2000 Server Resource Kit Distributed Systems Guide*. For more information about the components and features of third-party certificate services, contact the appropriate vendor for the certificate service.

Designing Your Public Key Infrastructure

With Windows 2000, you can design a PKI that meets a wide range of public key security needs. The needs must be determined in order to design and scale the infrastructure that will support them.

Identify Your Certificate Requirements

Before you can determine what PKI certificate services are needed, you must identify the applications you want to deploy that require digital certificates. You must also identify all uses for certificates, what users, computers, and services will require certificates, and what types of certificates you intend to issue. You can deploy Microsoft Certificate Services, or you can obtain other certificate services to support your public key needs. Identify the categories of users, computers, and services that will need certificates and determine the following information for each category:

- Name or description
- Reason certificates are needed
- Number of entities (users, computers, or services)
- Location of users, computers, and services

You need to provide certificate services to support the identified categories for each business unit and location in your organization. The certificate services you deploy are determined by the types of certificates to be issued, the number of entities that need certificates, and where the groups are located. For example, you might be able to deploy two issuing CAs to provide certificates for all the administrator groups in your organization. However, since there are many more business users than administrators in your organization, you might need to deploy separate issuing CAs in each facility to meet the needs of business users.

For more information about security solutions that use digital certificates, see "Choosing Security Solutions That Use Public Key Technology" in the *Microsoft Windows 2000 Server Resource Kit Distributed Systems*

Guide.

Basic Security Requirements for Certificates

Several basic factors affect overall security when you use certificates. For the certificates you intend to use, specify the requirements for the following factors:

- **Length of the private key.** In a typical deployment, user certificates have 1,024-bit keys and root CAs have 4,096-bit keys.
- **Cryptographic algorithms that are used with certificates.** The default algorithms are recommended.
- **Lifetime of certificates and private keys and the renewal cycle.** Certificate lifetimes are determined by the type of certificate, your security requirements, standard practices in your industry, and government regulations.
- **Special private key storage and management requirements.** For example, storage on smart cards and nonexportable keys.

The standard settings for certificates issued by Microsoft Certificate Services can meet typical security needs. However, you might want to specify stronger security settings for certificates that are used by certain user groups. For example, you can specify longer private key lengths and shorter certificate lifetimes for certificates used to provide security for very valuable information. You can also specify the use of smart cards for private key storage to provide additional security.

Determining Which Certificate Types to Issue

Identify the types of certificates you intend to issue. The types of certificates you issue depend on the certificate services you deploy and the security requirements you have specified for the certificates you intend to issue. You can issue certificate types that have multiple uses and that meet different security requirements.

For enterprise CAs, you can issue a variety of certificate types based on certificate templates and account privileges in a Windows 2000 domain. You can configure each enterprise CA to issue a specific selection of certificate types. Table 12.2 lists the different types of certificate templates available, and their purposes.

Table 12.2 Certificate Templates and Purposes

Certificate template name	Certificate purposes	Issued to
Administrator	Code signing, Microsoft trust list signing, EFS, secure e-mail, client authentication	People
Certification authority	All	Computers
ClientAuth	Client authentication (authenticated session)	People
CodeSigning	Code signing	People
CTLSigning	Microsoft trust list signing	People
Domain Controller	Client authentication, server authentication	Computers
EFS	Encrypting File System	People
EFSRecovery	File recovery	People
EnrollmentAgent	Certificate request agent	People
IPSECIntermediateOffline	IP Security	Computers
IPSECIntermediateOnline	IP Security	Computers
MachineEnrollmentAgent	Certificate request agent	Computers
Machine	Client authentication, server authentication	Computers
OfflineRouter	Client authentication	Computers/routers
SmartcardLogon	Client authentication	People
SmartcardUser	Client authentication, secure e-mail	People
SubCA	All	Computers
User	Encrypting File System, secure e-mail, client authentication	People

UserSignature	Secure e-mail, client authentication	People
WebServer	Server authentication	Computers
CEP Encryption	Certificate request agent	Routers
Exchange Enrollment Agent (Offline Request)	Certificate request agent	People
Exchange User	Secure e-mail, client authentication	People
Exchange User Signature	Secure e-mail, client authentication	People

For stand-alone CAs, you can specify certificate uses in the certificate request. You can also use custom policy modules to specify the certificate types to be issued for stand-alone CAs. For more information about developing custom applications for Microsoft Certificate Services, see the Microsoft Platform SDK link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .

The types of certificates issued by third-party certificate services are determined by the specific features and functions of each third-party product. For more information, contact the vendor for the certificate service.

Define Certificate Policies and Certification Authority Practices

You can use Microsoft Certificate Services or other certificate services to create CAs for your organization. Before deploying CAs, define the certificate policies and certificate practice statements (CPSs) for your organization. A certificate policy specifies what a certificate should be used for, and the liability assumed by the CA for this use. A certificate practice statement specifies the practices that the CA employs to manage the certificates it issues. A CPS describes how the requirements of the certificate policy are implemented in the context of the operating policies, system architecture, physical security, and computing environment of the CA organization. For example, a certificate policy might specify that the private key cannot be exported, so the CPS describes how this is accomplished by the PKI that you deploy.

Certificate Policies

Certificate policies can include the following types of information:

- How users will be authenticated to the CA
- Legal issues, such as liability, that might arise if the CA becomes compromised or is used for the wrong purpose
- What purposes the certificate can be used for
- Private key management requirements, such as requiring storage on smart cards or other hardware devices
- Whether the private key can be exported
- Requirements for users of the certificates, including what users must do in case their private keys are lost or compromised
- Requirements for certificate enrollment and renewal
- Certificate lifetime
- Cryptographic algorithms to be used
- Minimum length of the public key and private key pairs

Certificate Practices Statements (CPS)

A CPS for a certification authority can meet the requirements of multiple certificate policies. Each CPS contains information specific to that CA. However, the CPS for a subordinate CA can refer to the CPS of a parent CA for general or common information. A CPS can include the following types of information:

- Positive identification of the CA (including CA name, server name, and DNS address)
- What certificate policies are implemented by the CA and what certificate types are issued
- Policies, procedures, and processes for issuing and renewing certificates
- Cryptographic algorithms, CSP, and key length used for the CA certificate
- Lifetime of the CA certificate
- Physical, network, and procedural security of the CA
- The certificate lifetime of each certificate 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 CRL distribution points and publishing intervals
- Policy for renewing the CA's certificate before its expiration

Define Certification Authority Trust Strategies

Before deploying a Windows 2000 PKI, you need to define the CA trust strategies you want to use in your organization. With Windows 2000, you can establish trust for CAs using hierarchical CA trust chains and certificate trust lists.

Benefits of Certification Authority Trust Hierarchies

The Windows 2000 PKI has a hierarchical CA model. A CA hierarchy provides scalability, easy administration, and consistency with a growing number of third-party CA products.

In general, a hierarchy will contain multiple CAs with clearly defined parent-child relationships. In this model, subordinate CAs (children) are certified by (parent) CA-issued certificates, which bind a CA's public key to its identity.

The CA at the top of a hierarchy is referred to as a root CA. The CAs below the root in the hierarchy are referred to as subordinate CAs. In Windows 2000, if you trust a root CA (by having its certificate in your Trusted Root Certification Authorities store), you trust every subordinate authority in the hierarchy, unless a subordinate authority has had its certificate revoked by the issuing CA or has an expired certificate. Thus, any root CA is a very important point of trust in an organization and should be secured and maintained accordingly.

The advantage of this model is that verification of certificates requires trust in only a small number of root CAs. At the same time, it provides flexibility in terms of the number of certificate-issuing subordinate CAs. There are several practical reasons for deploying multiple subordinate CAs. These include:

Usage. Certificates can be issued for a number of purposes (for example, secure e-mail, network authentication, and so on). The issuing policy for these uses might be distinct, and separation provides a basis for administering these policies.

Organizational divisions. There can be different policies for issuing certificates, depending upon an entity's role in the organization. Again, you can create subordinate CAs to separate and administer these policies.

Geographic divisions. Organizations might have entities at multiple physical sites. Network connectivity between these sites might dictate a requirement for multiple subordinate CAs to meet usability requirements.

Multiple trust hierarchies also provide the following administrative benefits:

- Flexible configuration of the CA security environment (key strength, physical protection, protection against network attacks, and so on). You can tailor the CA environment to provide a balance between security and usability. For example, for a root CA, you can use special-purpose cryptographic hardware, maintain it in a locked vault, and operate it in offline mode. However, for an issuing CA, this same setup would be costly, make the CA difficult to use, and reduce the performance and effectiveness of the CA.
- The ability to frequently renew keys and certificates for those intermediate and issuing CAs that are at high risk for compromise, without requiring a change to established root trust relationships.
- The ability to turn off a subsection of the CA hierarchy without affecting established root trust relationships or the rest of the hierarchy.

In addition, deploying multiple issuing CAs provides the following benefits:

- Separate certificate policies for different categories of users and computers, or for organizational and geographic divisions. You can set up an issuing CA to provide certificates to each distinct category, department, or site.
- Distribution of certificate load and provision of redundant services. You can deploy multiple issuing CAs to distribute the certificate load to meet site, network, and server requirements. For example, slow or noncontinuous network links between sites can require issuing CAs at each site to meet certificate services performance and usability requirements. You can deploy issuing CAs to distribute certificate load as necessary to meet all site and network connectivity and load requirements. You can also deploy multiple issuing CAs to provide duplicate services. So if one CA fails, another issuing CA is available to provide uninterrupted service.

Benefits of Certificate Trust Lists

A certificate trust list is a list of self-signed certificates for the CAs whose certificates are to be trusted by your organization. A certificate trust list allows you to control the purpose and validity period of certificates issued by external certification authorities beyond what the certification authority specifies. Whenever you create a certificate trust list, you need to authorize it by signing the certificate trust list with a certificate issued by an already trusted certification authority.

There can be multiple certificate trust lists existing for a site. Because the uses of certificates for particular domains or organizational units (OUs) can be different, you can create certificate trust lists to reflect these uses, and assign a particular certificate trust list to a particular Group Policy object.

When you apply the Group Policy object to a site, domain, or OU, the policy is inherited by the corresponding computers. These computers then trust the CAs in the certificate trust list. You can also place the root CAs into Group Policy. Certificate trust lists are more convenient than using Group Policy because they expire.

You can create Windows 2000 certificate trust lists to provide the following benefits:

- **Creation of trust certificates from specific CAs without requiring broader trust for the root CA.** For example, you can use certificate trust lists on an extranet to trust certificates issued by certain commercial CAs. Users with certificates issued by the trusted commercial CAs can be granted permission to access restricted extranet resources by mapping the certificate to an account stored in Active Directory.
- **Restriction of the permitted use of certificates issued by trusted CAs.** For example, certificates issued by a CA might be valid for secure e-mail, network authentication, and signing software code. However, you can use a certificate trust list on an extranet to restrict the permitted use of certificates to secure mail only.
- **Control over how long third-party certificates and CAs are valid.** For example, a business partner's CA can have a lifetime of five years and issue certificates with lifetimes of one year. However, you can create a certificate trust list with a lifetime of six months to limit the time that certificates issued by the business partner's CA are trusted on your extranet.

Additional Considerations for Certification Authority Trust Strategies

Keep the following considerations in mind when defining your CA trust strategies:

- The depth of CA trust hierarchies is typically four levels (root CA, intermediate CA, issuing CA, and issued certificates).
- Third-party CAs can form all or part of the CA trust hierarchies, but to ensure that third-party CAs will provide the expected interoperability, test your proposed hierarchies in the lab.
- Some third-party products might require other CA trust models that might not be interoperable with rooted CA hierarchies. Windows 2000 and most commercial CAs support rooted CA hierarchies.

Define Security Requirements for Certification Authorities

You should define the security requirements to be provided for CAs. The security requirements for CAs can include the following:

- Using a hardware-based CSP for root CAs
- Maintaining root CAs in locked vaults
- Operating root CAs and sometimes intermediate CAs offline
- Keeping intermediate CAs and issuing CAs in secure data centers
- Longer keys for root certification authorities and high-level intermediate certification authorities

You can have an offline intermediate CA if you want to delegate authority from a parent company to a large number of separate organizations. You can then provide a subordinate CA for the subsidiary companies to keep offline.

Deciding on the security required for a CA involves determining a balance between the costs of implementing and maintaining security, and the risks of attack on the CA and the costs of a CA compromise. Higher risks of attacks on the CA and higher costs of a CA compromise justify higher costs for security measures to protect the CA. You should generally provide the most protection for root CAs, as well as provide more protection for intermediate CAs than for issuing CAs.

Protection for the root CA does not have to be expensive, especially for small companies. It might be adequate to have an offline root CA in a secure computer cabinet or to use removable media stored in a vault. The root CA computer should not have a network adapter.

Define Certificate Life Cycles

The certificate life cycle includes the following events:

- CAs installed and the certificates issued to them
- Certificates issued by CAs
- Certificates revoked (as necessary)
- Certificates renewed or expired

- CAs' certificates renewed or expired

You normally define the certificate life cycle to require periodic renewal of issued certificates. Issued certificates expire at the end of their lifetime and can be renewed in a cycle until revoked or expired, or until an issuing CA is unavailable. Each CA can issue certificates through several certificate renewal cycles until the CA approaches the end of its lifetime. At that time, the CA would either be retired because its keys are no longer useful, or the CA would be renewed with a new key pair.

You should define certificate life cycles that meet your business goals and security requirements. The life cycles you choose depend on various considerations, such as the following:

Length of private keys for CAs and issued certificates. In general, longer keys support longer certificate lifetimes and key lifetimes.

Security provided by the CSP. Typically, a hardware-based CSP is more difficult to compromise than a software-based CSP, and thus can support longer certificate lifetimes and key lifetimes.

Strength of the technology used for cryptographic operations. Some cryptographic technologies provide stronger security as well as support for stronger cryptographic algorithms. You can also use FORTEZZA Crypto Cards to provide stronger security than standard smart cards. Generally, cryptographic technology that is harder to break supports longer certificate lifetimes.

Security provided for CAs and their private keys. In general, the more physically secure the CA and its private key, the longer the CA lifetime.

Security provided for issued certificates and their private keys. For example, private keys stored on smart cards can be considered more secure than private keys stored as files on local hard disks because smart cards cannot be coerced to export the private key.

Risk of attack. The risk of attack depends on how secure your network is, how valuable the network resources protected by the CA trust chain are, and the cost of starting an attack.

How much trust you have for users of certificates. In general, lower trust requires shorter lifecycles and shorter key lifetimes. For example, you might trust temporary users less than normal business users, so you might issue temporary users' certificates with shorter lifetimes; you can also require stricter controls for renewal of temporary users' certificates.

The amount of administrative effort you are willing to devote to certificate renewal and CA renewal. For example, to reduce the administrative effort required to renew CAs, you can specify long, safe lifetimes for your certification trust hierarchies.

Give careful consideration to how long you want CAs and issued certificates and keys to be trusted. The longer the certificates and private keys are valid, the greater the risk and potential for a security compromise.

You should define certificate life cycles that realistically balance your business goals with your security requirements. Unrealistically short life cycles can result in excessive administrative efforts required to maintain the life cycles. Unrealistically long life cycles increase the risk of security compromises.

When you renew certificates using Microsoft CSP, you can also renew the certificate's key pair. In general, the longer the key pair is in use, the higher the risk of the key becoming compromised. You should establish maximum allowable key lifetimes and renew certificates with new key pairs before these limits are exceeded.

After you define a life cycle, you can change it later by renewing CAs, certificates, or keys at different periods than you originally specified. For example, if you later decide that the lifetime of the root CA places the CA at greater risk of compromise than you originally estimated, you can renew the CA chain and adjust the life cycle as necessary to mitigate risks.

Define Certificate Enrollment and Renewal Processes

Define the certificate enrollment and renewal processes that you will use for your organization. Microsoft Certificate Services supports the following certificate enrollment and renewal methods:

- Interactive certificate requests with the Certificate Request wizard (for Windows 2000 users, computers, and services only).
- Automatic certificate requests with the Automatic Certificate Request setup wizard (for Windows 2000 computer certificates only).
- Interactive certificate requests with the Microsoft Certificate Services Web pages (for most Web browser clients).
- Smart card enrollment with the Smart Card Enrollment Station.
- Custom certificate enrollment and renewal applications using Microsoft Enrollment Control.

The certificate enrollment and renewal process that you choose is determined by the users and computers for which you intend to provide services. You can use the Certificate Request wizard only for Windows 2000 clients. However, you can use Web-based enrollment and renewal services for most clients with Web browsers.

You can use the Microsoft Certificate Services Web pages as they are, or you can customize the pages. For example, you can limit user options or provide additional links to online user instructions and user support information.

Define Certificate Revocation Policies

The certificate revocation policies of your organization include policies for revoking certificates and policies for certificate revocation lists (CRLs).

Policies for Revoking Certificates

Your certificate revocation policy specifies the circumstances that justify revoking a certificate. For example, you can specify that certificates must be revoked when employees are terminated or transferred to other business units. You can also specify that certificates must be revoked if users misuse their security privileges or the private keys are compromised (a lost smart card, for instance). For computer certificates, you can specify that certificates must be revoked if the computer is replaced or permanently removed from service, or if the key is compromised.

Policies for Certificate Revocation Lists

Your CRL policies specify where you will distribute CRLs and the publishing schedule for CRLs. For example, you can specify that certain CRLs will be distributed to commonly used public folders and Web pages, as well as to Active Directory. You can also specify that certain CRLs be published daily instead of using the default weekly publication.

Define Maintenance Strategies

Define your maintenance and disaster recovery strategies for CAs. Maintenance and disaster recovery strategies include the following:

- Types of backups you will perform for CAs
- Schedules for conducting backups of CAs
- Policies for restoring CAs
- Policies for EFS recovery agents
- Policies for secure mail recovery

Developing Recovery Plans

You can develop recovery plans to help restore CAs if certificate services fail or CAs are compromised. Test recovery plans to ensure that they work as intended, and train your administrative staff how to use the recovery plans.

Recovery plans can include the following:

- Recovery procedures and checklists for administrators to follow
- Recovery toolkits or pointers to the toolkits
- Contingency plans

For more information about backup and recovery in Windows 2000, see "Determining Windows 2000 Storage Management Strategies" in this book.

Failed Certification Authority

A CA can fail for a variety of reasons, such as a server hard drive failure, a failed network adapter, or a server motherboard failure. Some failures can be quickly corrected by locating and correcting the problem with the CA server. For example, you can replace a failed network adapter or a failed motherboard and restart the computer to restore certificate services.

If a hard disk has failed, you can replace the hard disk and restore the server and the CA from the most recent backup set. If the CA is damaged or corrupted, you can restore the CA from the most recent backup set on the server.

If you must replace the server, configure the new server with the same network name and IP address as the failed CA server. You can then use Windows 2000 Backup or the Certification Authorities Restore wizard to restore the CA from the most recent backup set.

Compromised Certification Authority

When a CA has been compromised, you must revoke the CA's certificate. Revoking a CA's certificate invalidates

the CA and its subordinate CAs, as well as invalidating all certificates issued by the CA and its subordinate CAs. If you discover a compromised CA, perform the following activities as soon as possible:

- Revoke the compromised CA's certificate. If the CA has been renewed, revoke all of the CA's certificates only if all related keys have been compromised.
- Publish a new CRL containing the revoked CA certificate. Note that client applications can store the CRL until it expires, so you will not see the newly published CRL until the old one expires.
- Remove compromised CA certificates from Trusted Root Certification Authorities stores and CTLs.
- Notify all affected users and administrators of the compromise and inform them that certificates issued by the affected CAs are being revoked.
- Repair whatever led to the compromise.

To restore the CA hierarchy, you must deploy new CAs, or renew a CA's certificate and generate a new key to replace the compromised hierarchy. You must then reissue the appropriate certificates to users, computers, and services. Depending on where in the hierarchy the revocation occurred, it could require a new CA hierarchy or only a portion of it.

Developing Optional Custom Applications

You can deploy a wide variety of public key security solutions with the standard components and features of Windows 2000 PKI. However, you can also develop custom applications using the Microsoft CryptoAPI.

Using CryptoAPI, you can develop Custom Policy modules and custom exit modules to integrate certificate services with existing databases and third-party directory services. For example, you can develop an application that validates certificate requests from user information contained in an existing database or a third-party directory service.

You can also develop a custom application that uses special types of certificates. For example, you can develop an application that creates a digital thumbprint of an electronic document and then stores the thumbprint in a time- and date-stamped certificate. You can maintain these stamped certificates in a document registry database to provide integrity for the original document contents. When a document is compared to the digital thumbprint in the registry database, any tampering or modifications to the document since it was registered will be identified. You can use a document registry like this to provide an online, quality-assurance audit trail for products you manufacture, and thus ensure the integrity of electronic test and certification documentation.

In addition, you can develop a custom certificate enrollment and renewal application with Active Server Pages. For example, you can modify the standard Microsoft Certificate Services Web pages to add or delete features. You can also develop custom Web pages that integrate with third-party services or other applications that you develop.

For more information about developing custom applications for Microsoft Certificate Services, see the Microsoft Platform SDK link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .

Performing Resource Planning

You should estimate the network, computing, and facilities resources required to support the certificate services you intend to deploy in your organization. The total number of resources required can vary considerably depending on the size of your organization and the level and scope of the PKI you deploy.

When estimating resources, consider the resources required to support short-term needs and projected long-term growth of your organization.

The network and computing resources required for deployment include the following:

- Server computers that run certificate services and custom applications
- Cryptographic hardware, such as crypto-accelerator boards
- Hard disk storage for the certificate database and custom applications
- Storage resources for backups of CAs and custom applications
- Disaster recovery resources, such as recovery kits and hot-standby replacement servers

Certificate services performance can vary considerably depending on the following factors:

- **Length of the CA key used to sign certificates.** The longer the key, the more processing power and time are required to sign a certificate. It should be noted that a signing operation is performed (on the server) once per certificate at the time of issuance, while a verification operation is performed many times throughout the lifetime of a certificate (on the client or another server, depending on the protocol). Note that signing a certificate is more expensive than verifying it.
- **Complexity of the certification authority policy module logic used to validate certificate requests.** The more complex the policy logic, the longer it takes to process and issue certificates. Most people will find the Windows 2000 enterprise and stand-alone policy module sufficient. If you want to

develop a custom policy module, the cost of complexity should be considered both in the policy module and the exit module.

- **Performance impact of custom applications.** Custom applications affect the overall performance of certificate applications. For example, a certificate enrollment application that uses standard Common Gateway Interface (CGI) scripts can add significant delays to the enrollment process.

The hard disk capacity required to support the certificate databases depends on the following factors:

- **How many certificates are issued by the CA.** Project how many certificates will be issued for the life of the CA. A CA that issues a large number of certificates or that has a longer lifetime will require a larger certificate database.
- **The size of each certificate.** The certificate database includes all information in the certificates, including the public keys. Certificates that have larger public keys and that contain additional special information will consume more disk space per certificate issued.

Some large certificate databases might be several gigabytes or more. However, significantly smaller certificate databases are not normally expected to exceed several hundred megabytes in size. You should measure representative certificate database sizes in the lab and then extrapolate future database sizes based on the projected number of certificates you expect each CA to issue in its lifetime.

Deploying Your Public Key Infrastructure

After your public key design and deployment strategies have been validated and refined by pilot programs, you can deploy the PKI into your production environment. The following list shows a basic production rollout process that you can use to deploy your PKI.

Deploying the PKI includes the following activities:

- Scheduling production rollout in stages
- Providing training and support for production users
- Installing CAs
- Installing and configuring support systems or applications
- Configuring the certificates to be issued
- Configuring publication of certificate revocation lists
- Configuring public key Group Policy
- Configuring certificate renewal and enrollment
- Issuing certificates to users, computers, and certification authorities

Schedule Production Rollout in Stages

For large enterprise deployments, schedule the public key production rollout in stages. You can roll out different portions of the infrastructure as necessary to support your security goals and business needs.

For example, you might begin with EFS and IPSec features because you do not have to establish a CA hierarchy to get the security benefits of these features. You might place the next highest priority on secure mail and smart card authentication. You can choose to schedule rollout of the secure mail infrastructure before rollout of the smart card infrastructure, or you can choose to schedule secure mail to one group or site and simultaneously roll out the smart card infrastructure to another group or site.

To roll out the PKI for secure mail, you can schedule the following activities for each stage of the rollout:

- Install root CAs for secure mail in the parent domains for each tree in your organization (root CAs are used to certify intermediate CAs in that domain or a subdomain).
- Install and configure secure mail system and services (as necessary).
- Install intermediate CAs for secure mail in the domains or subdomains for each business unit (each business unit certifies and installs issuing CAs for its user groups).
- Install and configure issuing CAs (certified by the business unit) and certificate enrollment services in the domains or subdomains for user groups at each site, as necessary.

To roll out the PKI for smart cards, you can schedule the following activities for each stage of the rollout:

- Install root CAs for smart cards in the parent domains for each tree in your organization (root CAs are used to certify intermediate CAs in that domain or a subdomain).
- Install and configure smart card readers for users and smart card administrators.
- Install intermediate CAs for smart cards in the domains or subdomains for each business unit (each business unit certifies and installs issuing CAs for its user groups).

- Install and configure issuing CAs (certified by the business unit) and smart card enrollment stations in the domains or subdomains for user groups at each site, as necessary.

In addition, you can schedule the rollout of other portions of the PKI to support additional public key security functions such as secure Web communications and secure Web sites, software code signing, IPSec authentication, and EFS user and recovery operations.

Install Certification Authorities

You must install the CA hierarchies necessary to provide the required certificate services for your organization. You install the root CA first and then each subordinate CA in the hierarchy. For example, to create a three-level CA hierarchy and trust chain, you install CAs on server computers in the following order:

1. Root CA
2. Intermediate CAs
3. Issuing CAs

The root CA certificate is self-signed. Each subordinate CA is certified (issued its certificate) by the parent CA in the hierarchy. In the example of a three-level certificate hierarchy, each intermediate CA is certified by the root CA and each issuing CA is certified by an intermediate CA in the hierarchy.

Note It is possible for an intermediate CA to be certified by another intermediate CA, creating a deeper hierarchy.

You can install enterprise CAs, stand-alone CAs, or third-party CAs to create the required trust chains. To create a Windows 2000 Server CA, use the **Add/Remove Software wizard** in Control Panel to add Microsoft Certificate Services to each CA server.

During installation of Windows 2000 Server subordinate CAs, you can request the subordinate CA certificate from an online CA, or you can save the certificate request to a request file and make the certificate request offline. If you make an offline CA certificate request, the CA is not certified. You must manually use the Certification Authority MMC snap-in to import the CA's certificate and complete the CA installation after the certification authority's certificate has been issued by the parent CA. You can also use the same snap-in to import subordinate CA certificates issued by third-party parent CAs.

Install and Configure Supporting Systems and Applications

You must install any systems or applications required to support the PKI. Supporting systems and applications can include:

- Smart card readers at local computers
- Secure e-mail and key management systems
- Custom policy and exit modules
- Custom certificate enrollment and renewal applications
- Third-party PKI and certificate services
- Hardware-based cryptographic cards for acceleration and key storage on servers

Configure Certificates to Be Issued

By default, Windows 2000 enterprise CAs are installed ready to issue several certificate types. You can modify the default configuration by using the Certification Authority MMC snap-in to specify the certificate types to be issued by each CA. You can delete default certificate types that you do not want the CA to issue. You can also add more certificate types for the CA to issue.

Examples of Configurations

You can configure CAs to support multiple security functions or only one security function. Following are some ways you can configure CAs:

- For a root CA or an intermediate CA, you can configure the CA so it can issue subordinate certification authority certificates only.
- For an issuing CA that supports secure Web communication services, you can configure the CA so it can issue authenticated session, computer, and Web server certificates only.
- For an issuing CA that supports general business users, you can configure the CA so it can issue user certificates only. Likewise, you can configure a CA that supports administrators to issue administrator certificates only.
- For an issuing CA that supports smart card enrollment, you can configure the CA so it can issue smart card logon and smart card user certificates only.

Security Access Control Lists for Certificate Templates

Permission to request certificate types is controlled by the security access control lists for each certificate template. An enterprise CA grants certificate requests only for users, computers, or services that have the Enroll permission selected in the security access control list for that certificate template. The security access control lists for certificate templates are preconfigured to enable various default user accounts and security groups to enroll for certificate types.

You can use the Active Directory Sites and Services MMC snap-in to modify the security access control lists for each certificate template.

To modify the security access control lists for each certificate template

1. On the **View** menu, click **Show Services Node**.
2. Expand the Services node and the Public Key Services and Certificate Templates containers.
3. Select a certificate template in the details pane and click the **Security** tab of its Properties sheet. This tab shows the groups that have access to this template, and the specific permissions of each group.

For example, by default, only members of the Domain Administrators security group can request and obtain enrollment agent certificates. However, to specify that only certain members of your security department can request and obtain enrollment agent certificates, you can change the security access control list for the enrollment agent certificate template. You can remove domain admins from the access control list and add the appropriate user accounts or security groups.

For Windows 2000 stand-alone CAs, information about the certificate type must be included in the certificate request because stand-alone CAs do not use certificate templates. You can use stand-alone CAs with custom policy modules and custom certificate request applications to control the types of certificates that are issued.

Configure Certificate Revocation List Publication

By default, enterprise CAs publish CRLs weekly to Active Directory. By default, stand-alone and enterprise CAs publish CRLs weekly to a directory on the CA server. You can use the Certification Authority MMC snap-in to modify the point at which the CRL is distributed. You can also use the Certification Authority snap-in to interactively publish a new CRL or to change the publication schedule.

Configure Public Key Group Policy

You can use the Group Policy MMC snap-in to configure public key Group Policy for sites, domains, and organizational units. You can configure the following optional categories of public key policy:

EFS Recovery Agents

By default, the local Administrator user account for the first domain controller installed in the domain is the EFS recovery account for that domain. You can specify alternate encrypted data recovery agents for EFS by importing the appropriate alternate agent's EFS recovery agent certificate into policy. Therefore, you must first issue EFS recovery agent certificates to the user accounts on the local computers that you want to use as alternate recovery agents.

Automatic Certificate Enrollment

You can specify automatic enrollment and renewal for computer certificates. When automatic enrollment is configured, the specified certificate types are issued to all computers within the scope of the public key Group Policy. Computer certificates issued by automatic enrollment are renewed from the issuing CA. Automatic enrollment does not function unless at least one enterprise CA is online to process certificate requests.

For virtual private networks (VPNs) using IPSec with L2TP, remember to set up Group Policy to permit automatic enrollment for IPSec certificates. In Table 12.2, any Rivest-Shamir-Adleman (RSA)-signed certificate issued to a computer that is stored in the computer account can be used for IPSec. For more information about certificates for L2TP over IPSec VPN connections, see Windows 2000 Server Help.

Root Certificate Trust

When you install an enterprise root CA, the CA's certificate is added to the trusted root certification authorities for the domain. You can also interactively add certificates for other root CAs to the Trusted Root Certification Authorities container in the Group Policy MMC snap-in. The root CA certificates that you add become trusted root CAs within Group Policy. If you want to use a stand-alone CA or a third-party CA as a root CA in a certification hierarchy, you need to add the CA's certificate to the trusted root certification authorities container in Group Policy.

Certificate Trust Lists

You can create certificate trust lists to trust specific CAs and to restrict the uses of certificates issued by the CAs. For example, you can use a certificate trust list to trust certificates issued by a commercial CA and restrict

the permitted uses for those certificates. You can also use certificate trust lists to control trust on an extranet for certificates issued by CAs that are managed by your business partners.

For instance, your company might be engaged in a joint venture with another company. The partner company could issue its own certificates for Web access, secure e-mail, software signing, and so forth. You might want to exchange secure e-mail with employees of the partner company, but you do not want to issue certificates for this purpose. You can add the other company's root CA to a new certificate trust list in your enterprise trust container, specifying that the partner certificates will be trusted for e-mail only.

Configure Certificate Enrollment and Renewal

Microsoft Certificate Services supports a variety of enrollment and renewal methods, such as certificate requests with the Certificate Request wizard and certificate requests with the Microsoft Certificate Services Web pages. However, if you deploy third-party certificate services or custom certificate enrollment and renewal applications, you must perform any configuration required for those services and applications.

Start Issuing Certificates

When the required certificate services are installed and configured, you can start issuing certificates to users, computers, and services. Keep the following considerations in mind when you start to issue certificates:

- Certificates are issued for computers within the scope of the Automatic Certificate Request settings of the domain's Group Policy. Administrators can also manually request certificates for local computers with the Certificate Request wizard or the Microsoft Certificate Services Web pages. Consider scheduling manual enrollment in stages to help distribute the administrative workload for computer enrollment.
- Smart card administrators can start issuing smart card certificates with the Smart Card Enrollment Station available on the Microsoft Certificate Services Web pages. Consider scheduling smart card enrollment in stages to help distribute the administrative workload for smart card enrollment.
- During the transition to smart cards, you usually enable both smart card authentication and the CTRL+ALT+DEL secure logon sequence. However, because this weakens network security, configure user account policy to require smart cards to log on interactively as soon as smart card users are trained and are using their cards.

Monitor the performance of certificate services closely as you start issuing certificates to ensure that CAs handle the certificate load. To correct excessive load conditions, consider adding more issuing CAs or scheduling certificate enrollment in smaller stages. Certificate renewal might also produce excessive load conditions, so adding more CAs and scheduling certificate enrollment in smaller stages can also help distribute peak renewal loads.

Public Key Infrastructure Planning Task List

Table 12.4 summarizes the tasks you need to perform when planning PKI deployment.

Table 12.4 Public Key Infrastructure Planning Task List

Task	Location in chapter
Identify certificate requirements.	Identify Your Certificate Requirements
Define processes for issuing certificates.	Defining Certificate Policies and Certification Authority Practices
Define CA trust hierarchy.	Define Certification Authority Trust Strategies
Define security requirements for CAs.	Define Security Requirements for Certification Authorities
Define certificate life cycles.	Define Certificate Life Cycles
Define certificate enrollment and renewal processes.	Define Certificate Enrollment and Renewal Processes
Define certificate revocation policies.	Define Certificate Revocation Policies
Define maintenance policies.	Define Maintenance Strategies
Define disaster recovery strategies.	Developing Recovery Plans
Create a rollout plan and schedule.	Deploying Your Public Key Infrastructure

Send feedback to Microsoft
© Microsoft Corporation. All rights reserved.