Microsoft PKI Design Overview

Organizations use a variety of technology solutions to enable essential business processes, such as online ordering, exchanges of contracts, and remote access. A public key infrastructure based on Microsoft Windows Server 2003 Certificate Services provides a means by which organizations can secure these critical internal and external processes.

Deploying a PKI allows you to perform tasks such as:

1.	Digitally signing files such as documents and applications.
2.	Securing e-mail from unintended viewers.
3.	Enabling secure connections between computers, even if they are connected over the public Internet or through a wireless network.
4.	Enhancing user authentication through the use of smart cards.

If your organization does not currently have a public key infrastructure, begin the process of designing a new public key infrastructure by identifying the certificate requirements for your organization.

If your organization already uses a public key infrastructure based on older Microsoft products or third-party certificate services, you can improve your PKI capabilities by taking advantage of new and enhanced features in Windows Server 2003 products.

When you have completed the PKI design process, you can deploy a public key infrastructure that provides solutions for all of your internal security requirements, as well as security requirements for business exchanges with external customers or business partners.

Defining Certificate Requirements and Infrastructure

You can use a Windows Server 2003 public key infrastructure to provide a wide range of strong, scalable, cryptography-based solutions for

network and information security. The value of the information that you want to protect, as well as the costs involved with implementing a strong security system, impact the level of security that you choose for your organization.

To support the certificate-based applications of your organization, you must establish a framework of linked CAs that are responsible for issuing, validating, renewing, and revoking certificates as needed. The goal in establishing a CA infrastructure is to provide reliable service to users, manageability for administrators, and flexibility to meet both current and future needs, while maintaining an optimum level of security for the organization.

Figure 1.1 shows the steps that are involved in determining your certificate requirements and in designing your PKI infrastructure.

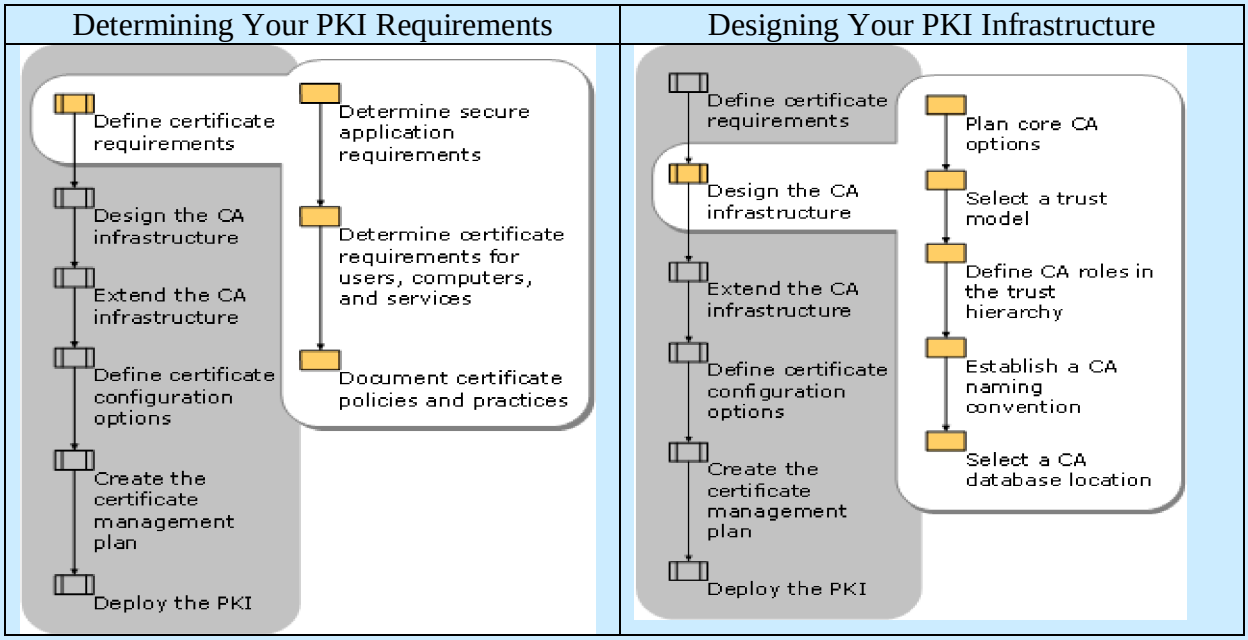


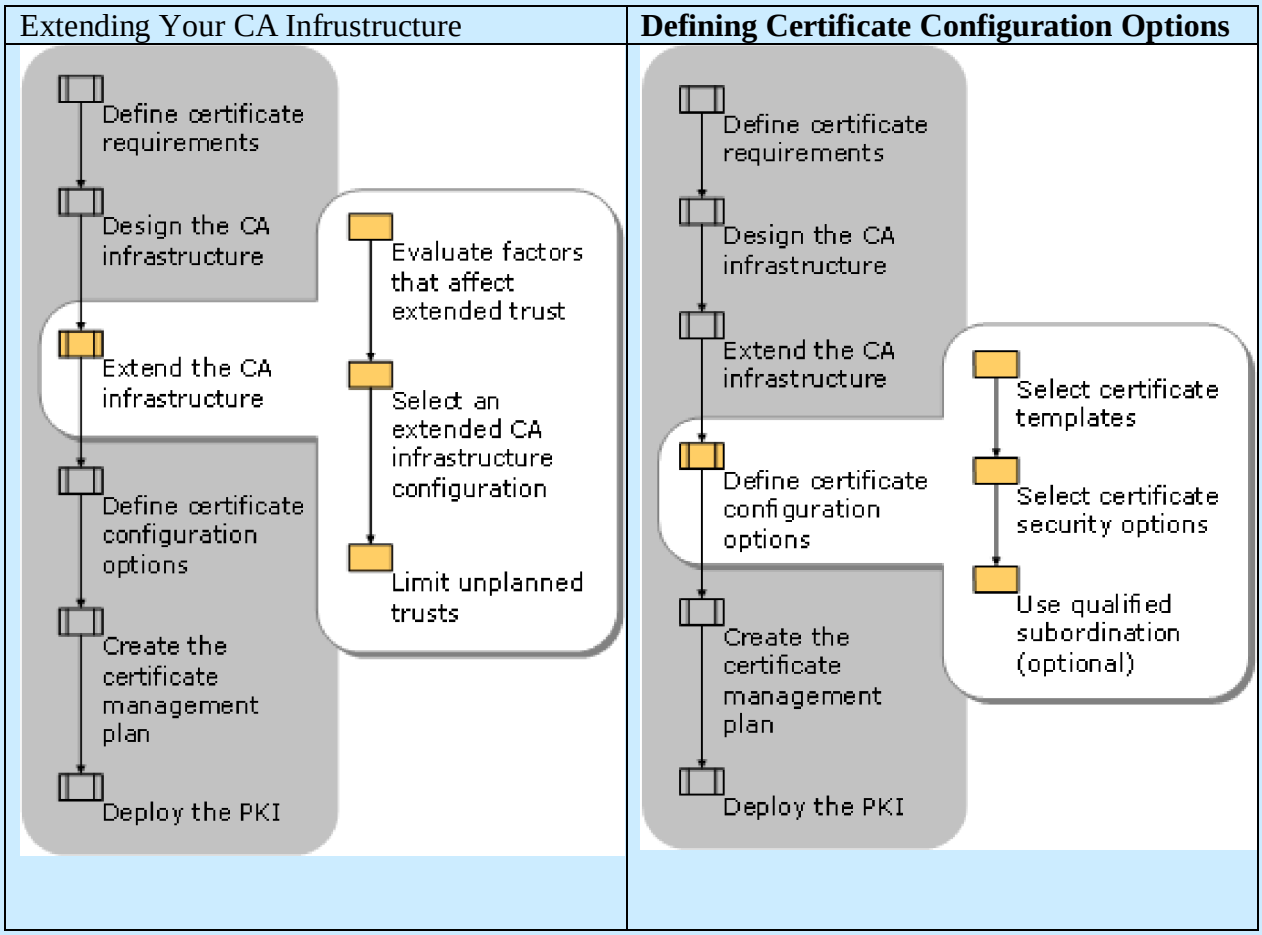
Figure 1.1 Defining Certificate Requirements

Extending Your CA Infrastructure and Defining Options

You can use a rooted CA hierarchy to enable many PKI applications. However, you might find that your PKI needs are too complex to be met by a simple rooted hierarchy. For example, you might need to extend your CA infrastructure to accommodate joint ventures, mergers, geographic, or other business requirements.

After your CA infrastructure is in place, you can begin to define the certificate configuration options that you need to meet the requirements of your users, as well as the security needs of your organization.

Figure 2 below shows the steps involved in extending your CA infrastructure and in defining certificate configuration options.



Creating You PKI Management Plan and Deploying It

After you have configured certificates for your organization, you need to create a plan for managing certificates throughout their lifetimes.

After your public key design has been validated and refined by lab testing and pilot programs, you can deploy the PKI in your production environment. A disciplined approach to deploying a PKI is absolutely essential in order to establish the security of the applications that you are enabling. Figure 16.21 shows the PKI deployment process.

Creating the Certificate Management Plan	Steps to Deploy Your PKI