Lesson 13

Configuring Active Directory Certificate Services

Knowledge Assessment

Fill in the Blank

Complete the following sentences by writing the correct word or words in the blanks provided.

1. The \_Network Device Enrollment Service\_ allows administrators to obtain PKI certificates for network infrastructure devices such as routers and switches.

2. One or more Online Responders can be chained together to form a(n) \_Responder array\_.

3. A(n) \_enterprise CA\_ is a CA that integrates with Active Directory and allows autoenrollment of user and computer certificates through the use of Group Policy and certificate templates.

4. For a user to log on to a workstation using a smart card, that workstation must be equipped with a(n) \_smart card reader\_.

5. The top-level CA in any PKI hierarchy is the \_root CA\_.

6. One alternative to public key cryptography is to use a(n) \_shared secret key\_.

7. Each PKI certificate consists of a public key that is widely known and a(n) \_private key\_ that is known only to the user or computer who holds the certificate.

8. Users can request certificates via the Web using the \_Certification Authority Web Enrollment\_ service.

9. To protect against lost or corrupted private keys, you can configure one or more users to function as a(n) \_key recovery agent\_ within AD Certificate Services.

10. You can manage many facets of the AD Certificate Services server role from the command line by using the \_certutil\_ utility.

Multiple Choice

Circle the correct choice.

1. Each PKI environment can have one and only one of the following:

a. Standalone CA

b. Enterprise CA

c. Root CA

d. Subordinate CA

Each Public Key Infrastructure is hierarchical, with a single root CA at the top and any number of subordinate CAs residing beneath the root CA.

2. Each server that functions as a CA must be configured with a(n):

a. Revocation configuration

b. Key Recovery Agent

c. User template

d. Online Responder

Each Certificate Authority in a PKI environment must have a revocation configuration, regardless of how many exist within an environment.

3. You can restrict enrollment agents so that they can only request certificates on behalf of specific users or computers based on:

a. OU membership

b. Security group membership

c. Name

d. Email address

Restricted enrollment agents are configured on the basis of security group memberships. You cannot restrict them based on Organizational Units.

4. To configure an offline root CA, your root CA must be configured as follows:

a. Standalone CA

b. Enterprise CA

c. Subordinate CA

d. Online Responder

To configure an offline root, the CA must be configured as a standalone CA and not an enterprise CA.

5. Certificate templates must be compatible with at least which operating system to allow autoenrollment?

a. Windows Server 2008

b. Windows 2000 Server

c. Windows Server 2003

d. Windows Vista Enterprise

Certificate autoenrollment is supported in Windows Server 2003 and Windows Server 2008, so any templates that allow this feature must be compatible with Windows Server 2003 or later.

6. A lost or corrupted private key can only be recovered by someone who has been issued a(n):

a. Key Recovery Agent certificate

b. Administrator certificate

c. Domain Controller certificate

d. Online Responder certificate

Key Recovery Agents are part of the private key escrow process that is available when AD CS is integrated with Active Directory.

7. An organization may have one or more of these to distribute the load of issuing certificates in a geographically dispersed organization:

a. Root CA

b. Enterprise CA

c. Standalone CA

d. Intermediate CA

The hierarchical nature of PKI allows you to deploy intermediate CAs to provide distributed load balancing for issuing certificates within an organization.

8. To authenticate using a smart card that has been configured for a user, the user must have the following installed at his workstation:

a. Smart card enrollment station

b. Online Responder

c. Smart card reader

d. Smart card enrollment agent

To deploy smart cards for user logons, each workstation using smart cards must have an installed smart card reader.

9. Which component of Active Directory Certificate Services uses the Online Certificate Status Protocol to respond to client requests?

a. NDES

b. Online Responder

c. Certificate Revocation List

d. Subordinate CA

The Online Responder uses the Online Certificate Status Protocol (OCSP) to respond to client requests for certificate status and revocation information.

10. Which of the following provides an alternative to the use of public key cryptography for secured communications?

a. Shared secret key

b. Online Certificate Status Protocol

c. Private key cryptography

d. Responder Arrays

Shared secret keys involve a fast and simple method of encryption, but it is difficult to deploy shared secret keys throughout an organization regardless of its size.

CASE SCENARIO

Scenario 13-1: Consulting for Contoso, Ltd.

You are a computer consultant for Kevin Browne, the Chief Security Officer (CSO) of Contoso, Ltd. Contoso, Ltd. has a single Active Directory domain structure with the domain contoso.com. Contoso, Ltd. has research contracts with numerous pharmaceutical companies worldwide—50 locations in 12 countries. Some Contoso offices have full T1 or T3 connectivity to the corporate headquarters office in Chicago, Illinois; other offices, however, connect via slow and sometimes heavily utilized satellite links. All Contoso servers are running Windows Server 2008, and all Contoso workstations are running Windows XP Professional or Windows Vista Enterprise.

Given the sensitive nature of the data that Contoso's researchers work with on a daily basis, Contoso's CSO wants to make it possible for researchers to encrypt their files and email messages against tampering by outsiders. Because some of the work requires Contoso to conform to government security standards in many countries, the CSO wishes to deploy this capability in the most secure manner possible. However, he is concerned about adding traffic to the already overburdened WAN links at some locations, because this would adversely affect the researchers' ability to perform their research.

Based on this information, answer the following questions regarding the recommendations that you would make to Contoso, Ltd.

1. To minimize the burden on Contoso Ltd's WAN links, how would you deploy CA computers within their environment?

Because the PKI structure is hierarchical, you can deploy a single root CA at the corporate headquarters, and then deploy multiple subordinate or intermediate CAs at remote locations that have concerns about their WAN utilization.

2. The Contoso, Ltd. CSO has read about the security benefits of deploying an offline root CA. To use this feature, how must you design the Contoso, Ltd. PKI infrastructure?

To allow an offline root, the Contoso, Ltd. PKI must use a standalone CA as the root CA.

3. The CSO wishes to deploy key archival capabilities in case a researcher's private key is lost or compromised. However, he is concerned about the possibility of a single malicious administrator abusing this privilege as a way to gain access to encrypted files. How can Contoso, Ltd. guard against this?

Set the number of recovery agents to be used to a number greater than 1, which will require intervention by more than one key recovery agent to recover a lost or compromised private key.