Microsoft® Official Course

Module 6
Implementing AD CS
Module Overview

• Using Certificates in a Business Environment
• PKI Overview
• Deploying CAs
• Deploying and Managing Certificate Templates
• Implementing Certificate Distribution and Revocation
• Managing Certificate Recovery
Lesson 1: Using Certificates in a Business Environment

• Using Certificates for SSL
• Using Certificates for Digital Signatures
• Demonstration: Signing a Document Digitally
• Using Certificates for Content Encryption
• Using Certificates for Authentication
Using Certificates for SSL

• The purpose of securing a connection with SSL is to protect data during communication
• For SSL, a certificate must be installed on the server
• Be aware of trust issues
• The SSL works in the following steps:
  1. The user types an HTTPS URL
  2. The web server sends its SSL certificate
  3. The client performs a check of the server certificate
  4. The client generates a symmetric encryption key
  5. The client encrypts this key with the server’s public key
  6. The server uses its private key to decrypt the encrypted symmetric key
• Make sure that you configure the SSL certificate properly
Using Certificates for Digital Signatures

• Digital signatures ensure:
  • Content is not modified during transport
  • The identity of the author is verifiable

• Digital signatures work in the following steps:
  1. When an author digitally signs a document or a message, the operating system on his or her machine creates a message cryptographic digest
  2. The cryptographic digest is then encrypted by using author’s private key and added to the end of the document or message
  3. The recipient uses the author’s public key to decrypt the cryptographic digest and compare it to the cryptographic digest created on the recipient’s machine

• Users need to have a certificate based on a User template to use digital signatures
Demonstration: Signing a Document Digitally

In this demonstration, your instructor will show you how to digitally sign a document in Microsoft Word
Using Certificates for Content Encryption

- Encryption protects data from unauthorized access
- EFS uses certificates for file encryption

To send an encrypted message, you must possess the recipient’s public key

<table>
<thead>
<tr>
<th>Header</th>
</tr>
</thead>
<tbody>
<tr>
<td>File encryption key: Encrypted with the file owner’s public key</td>
</tr>
<tr>
<td>File encryption key: Encrypted with the public key of Recovery agent 1</td>
</tr>
<tr>
<td>File encryption key: Encrypted with the public key of Recovery agent 2 (optional)</td>
</tr>
<tr>
<td>Encrypted Data</td>
</tr>
</tbody>
</table>

Data Recovery Fields
Using Certificates for Authentication

You can use certificates for user and device authentication, and in network and application access scenarios such as:

- L2TP/IPsec VPN
- EAP-TLS
- Protected Extensible Authentication Protocol
- NAP with IPsec
- Outlook Web App
- Mobile device authentication
Lesson 2: PKI Overview

• What Is PKI?
• Components of a PKI Solution
• What Are CAs?
• Overview of the AD CS Server Role in Windows Server 2012
• New Features of AD CS in Windows Server 2012
• Public vs. Private CAs
• What Is a Cross-Certification Hierarchy?
What Is PKI?

PKI:

• Is a standard approach to security-based tools, technologies, processes, and services that are used to enhance the security of communications, applications, and business transactions

• Relies on the exchange of digital certificates between users and trusted resources

PKI provides:

• Confidentiality
• Integrity
• Authenticity
• Nonrepudiation
Components of a PKI Solution

- CA
- Digital Certificates
- Certificate Templates
- CRLs and Online Responders
- Public Key–Enabled Applications and Services
- Certificates and CA Management Tools
- AIA and CDPs
What Are CAs?

Root CA

- Issues a self-signed certificate for itself
- Verifies the identity of the certificate requestor
- Issues certificates to users, computers, and services
- Manages certificate revocation
Overview of the AD CS Server Role in Windows Server 2012

- CA
- CA Web enrollment
- Online Responder
- NDES
- CES
- CEP
New Features of AD CS in Windows Server 2012

- All AD CS role services run on all versions of Windows Server
- Full integration with Server Manager
- Manageable through Windows PowerShell
- New certificate template version (v4)
- Support for automatic renewal of certificates for non-domain joined computers
- Enforcement of certificate renewal with the same key
- Additional security for certificate requests
- Support for Virtual Smart Cards
Internal private CAs:
• Require greater administration than external public CAs
• Cost less than external public CAs, and provide greater control over certificate management
• Are not trusted by external clients by default
• Offer advantages such as customized templates and autoenrollment

External public CAs:
• Are trusted by many external clients
• Have slower certificate procurement
What Is a Cross-Certification Hierarchy?

Cross-Certification at the Root CA Level

Root CA

Subordinate CA

Organization 1

Root CA

Subordinate CA

Organization 2

Cross-Certification Subordinate CA to Root CA

Root CA

Subordinate CA

Organization 1

Root CA

Subordinate CA

Organization 2
Lesson 3: Deploying CAs

- Options for Implementing CA Hierarchies
- Stand-Alone vs. Enterprise CAs
- Considerations for Deploying a Root CA
- Demonstration: Deploying a Root CA
- Considerations for Deploying a Subordinate CA
- How to Use the CAPolicy.inf File for Installation
- Configuring CA Administration and Security
- Configuring CA Policy and Exit Modules
- Demonstration: Configuring CA Properties
- CA Backup and Recovery
Options for Implementing CA Hierarchies

Policy CA Usage

Two-Tier Hierarchy

Cross-Certification Trust
<table>
<thead>
<tr>
<th>Stand-alone CAs</th>
<th>Enterprise CAs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Must be used if any CA (root/intermediate/policy) is offline, because a stand-alone CA is not joined to an AD DS domain</td>
<td>Requires the use of AD DS</td>
</tr>
<tr>
<td>Can use Group Policy to propagate certificate to trusted root CA certificate store</td>
<td>Publishes user certificates and CRLs to AD DS</td>
</tr>
<tr>
<td>Users provide identifying information and specify type of certificate</td>
<td>Issues certificates based upon a certificate template</td>
</tr>
<tr>
<td>Does not require certificate templates</td>
<td>Supports autoenrollment for issuing certificates</td>
</tr>
<tr>
<td>All certificate requests are kept pending until administrator approval</td>
<td></td>
</tr>
</tbody>
</table>
Considerations for Deploying a Root CA

• Computer name and domain membership cannot change

• When you plan private key configuration, consider the following:
  • CSP
  • Key character length with a default of 2,048
  • The hash algorithm that is used to sign certificates issued by a CA

• When you plan a root CA, consider the following:
  • Name and configuration
  • Certificate database and log location
  • Validity period
Demonstration: Deploying a Root CA

In this demonstration, you will see how to deploy an enterprise root CA
Considerations for Deploying a Subordinate CA

- S/MIME
- EFS
- RAS

- India
- Canada
- USA

- Load Balancing
- Employee
- Contractor
- Partner

Locations
Organizational Divisions
How to Use the CAPolicy.inf File for Installation

The CAPolicy.inf file is stored in the `%Windir%` folder of the root or subordinate CA, and defines the following:

- CPS
- Object Identifier
- CRL publication intervals
- CA renewal settings
- Key size
- Certificate validity period
- CDP and AIA paths
• You can establish role-based administration for the CA hierarchy by defining the following roles:
  • CA administrator
  • Certificate manager
  • Backup operator
  • Auditor
  • Enrollees

• You can assign the following permissions on the CA level:
  • Read
  • Issue and Manage Certificates
  • Manage CA
  • Request Certificates

• Certificate managers can be restricted to a template
Configuring CA Policy and Exit Modules

- The policy module determines the action that is performed after the certificate request is received.
- The exit module determines what happens with a certificate after it is issued.
- Each CA is configured with default policy and exit modules.
- The FIM CM 2010 deploys custom policy and exit modules.
- The exit module can send email or publish a certificate to a file system.
- You have to use certutil to specify these settings, as they are not available in the CA administrator console.
Demonstration: Configuring CA Properties

In this demonstration, your instructor will show you how to configure CA properties
CA Backup and Recovery

• To back up a CA, follow this procedure:
  1. Record the names of the certificate templates
  2. Back up a CA in the CA admin console
  3. Export the registry subkey
  4. Uninstall the CA role (optional, only if you move CA)
  5. Confirm the \%SystemRoot\% folder locations
  6. Remove the old CA from the domain (optional, only if you move CA)

• To restore, follow this procedure:
  1. Install AD CS
  2. Use the existing private key
  3. Restore the registry file
  4. Restore the CA database and settings
  5. Restore the certificate templates
Lab A: Deploying and Configuring a CA Hierarchy

- Exercise 1: Deploying a Stand-Alone Root CA
- Exercise 2: Deploying an Enterprise Subordinate CA

Logon Information
Virtual machines: 20412D-LON-DC1 20412D-LON-SVR1 20412D-LON-SVR2 20412D-LON-CA1

User name: Adatum\Administrator
Password: Pa$$w0rd

Estimated Time: 50 minutes
As A. Datum Corporation has expanded, its security requirements have also increased. The security department is particularly interested in enabling secure access to critical websites, and in providing additional security for features. To address these and other security requirements, A. Datum has decided to implement a PKI using the AD CS role in Windows Server 2012.

As one of the senior network administrators at A. Datum, you are responsible for implementing the AD CS deployment.
• Why is it not recommended to install just an enterprise root CA?
Lesson 4: Deploying and Managing Certificate Templates

- What Are Certificate and Certificate Templates?
- Certificate Template Versions in Windows Server 2012
- Configuring Certificate Template Permissions
- Configuring Certificate Template Settings
- Options for Updating a Certificate Template
- Demonstration: Modifying and Enabling a Certificate Template
A certificate contains information about users, devices, usage, validity, and a key pair

A certificate template defines:

- The format and contents of a certificate
- The process for creating and submitting a valid certificate request
- The security principals that are allowed to read, enroll, or use autoenrollment for a certificate that will be based on the template
- The permissions required to modify a certificate template
Certificate Template Versions in Windows Server 2012

Version 1:
- Introduced in Windows 2000 Server, provides for backward compatibility in newer versions
- Creates by default when a CA is installed
- Cannot be modified (except for permissions) or removed, but can be duplicated to become version 2 or 3 templates, which can then be modified

Version 2:
- Default template introduced with Windows Server 2003
- Allows customization of most settings in the template
- Several preconfigured templates are provided when a CA is installed

Version 3:
- Supports advanced Suite B cryptographic settings
- Includes advanced options for encryption, digital signatures, key exchange, and hashing
- Only supports Windows Server 2008 and Windows Server 2008 R2 servers
- Only supports Windows Vista and Windows 7 client computers

Version 4:
- Available only for Windows Server 2012 and Windows 8 clients
- Supports both CSPs and KSPs
- Supports renewal with the same key
# Configuring Certificate Template Permissions

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Control</td>
<td>Allows a designated user, group, or computer to modify all attributes—including ownership and permissions</td>
</tr>
<tr>
<td>Read</td>
<td>Allows a designated user, group, or computer to read the certificate in AD DS when enrolling</td>
</tr>
<tr>
<td>Write</td>
<td>Allows a designated user, group, or computer to modify all attributes except permissions</td>
</tr>
<tr>
<td>Enroll</td>
<td>Allows a designated user, group, or computer to enroll for the certificate template</td>
</tr>
<tr>
<td>Autoenroll</td>
<td>Allows a designated user, group, or computer to receive a certificate through the autoenrollment process</td>
</tr>
</tbody>
</table>
For each certificate template, you can customize several settings, such as validity time, purpose, CSP, private key exportability, and issuance requirements.

<table>
<thead>
<tr>
<th>Category</th>
<th>Single purpose examples</th>
<th>Multiple purpose examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td>• Basic EFS</td>
<td>• Administrator</td>
</tr>
<tr>
<td></td>
<td>• Authenticated session</td>
<td>• User</td>
</tr>
<tr>
<td></td>
<td>• Smart card logon</td>
<td>• Smart card user</td>
</tr>
<tr>
<td>Computers</td>
<td>• Web server</td>
<td>• Computer</td>
</tr>
<tr>
<td></td>
<td>• IPsec</td>
<td>• Domain controller</td>
</tr>
</tbody>
</table>
Options for Updating a Certificate Template

**Modifying**
Modify the original certificate template to incorporate the new settings

**Superseding**
Replace one or more certificate templates with an updated certificate template
Demonstration: Modifying and Enabling a Certificate Template

In this demonstration, you will see how to modify and enable a certificate template
Lesson 5: Implementing Certificate Distribution and Revocation

- Options for Certificate Enrollment
- How Does Autoenrollment Work?
- Enrollment Agent Overview
- Demonstration: Configuring the Restricted Enrollment Agent
- What Is NDES?
- How Does Certificate Revocation Work?
- Considerations for Publishing AIAs and CDPs
- What Is an Online Responder?
- Demonstration: Configuring an Online Responder
### Options for Certificate Enrollment

<table>
<thead>
<tr>
<th>Method</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autoenrollment</td>
<td>• To automate the request, retrieval, and storage of certificates for domain-based computers</td>
</tr>
<tr>
<td>Manual enrollment</td>
<td>• To request certificates by using the Certificates Templates console or Certreq.exe when the requestor cannot communicate directly with the CA</td>
</tr>
</tbody>
</table>
| CA Web enrollment     | • To request certificates from a website that is located on a CA  
                        | • To issue certificates when autoenrollment is not available |
| Enroll on behalf      | • To provide IT staff with the right to request certificates on behalf of another user (Enrollment Agent) |
How Does Autoenrollment Work?

A certificate template is configured to Allow, Enroll, and Autoenroll permissions for users who receive the certificates.

The CA is configured to issue the template.

An Active Directory Group Policy Object should be created to enable autoenrollment. The GPO should be linked to the appropriate site, domain, or organizational unit.

The client machine receives the certificates during the next Group Policy refresh interval.
Enrollment Agent Overview

An Enrollment Agent is a user who has the appropriate certificate assigned and has the ability to request certificates on behalf of other users or computers.

The restricted Enrollment Agent has limited permissions:

- Limits permissions of the Enrollment Agent:
  - For specific group of users
  - For specific certificate templates

- Requires Windows Server 2008 Enterprise edition or Windows Server 2012 CA
In this demonstration, you will see how to configure the Restricted Enrollment Agent
What Is NDES?

NDES:
- Uses SCEP to communicate with network devices
- Functions as an AD CS role service
- Requires IIS
How Does Certificate Revocation Work?

1. Certificate is revoked
2. Certificate revocation is published
3. Client computer verifies certificate validity and revocation
Considerations for Publishing AIAs and CDPs

Publish the root certificate CA and URL to:
AD DS
Web servers
FTP servers
File servers

External Web server

FTP server

AD DS

Offline Root CA

Internet
Firewall
Firewall

Internal Web server
File server
What Is an Online Responder?

- Uses OCSP validation and revocation checking using HTTP
- Receives and responds dynamically to individual requests
- Supports only Windows Server 2008, Windows Vista, and newer Windows operating systems
- Functions as a responder to multiple CAs
Demonstration: Configuring an Online Responder

In this demonstration, you will see how to configure an Online Responder
Lesson 6: Managing Certificate Recovery

• Overview of Key Archival and Recovery
• Configuring Automatic Key Archival
• Demonstration: Configuring a CA for Key Archival
• Recovering a Lost Key
• Demonstration: Recovering a Lost Private Key
Overview of Key Archival and Recovery

• Private keys can get lost when:
  • A user profile is deleted
  • An operating system is reinstalled
  • A disk is corrupted
  • A computer is lost or stolen
• It is critical that you archive private keys for certificates that are used for encryption
• The KRA is needed for key recovery
• Key archival must be configured on the CA and on the certificate template
• Key recovery is a two-phase process:
  1. Key retrieval
  2. Key recovery
• The KRA certificate must be protected
Steps to configure automatic key archival:

1. Configure and issue the KRA certificate template
2. Designate a person as the KRA, and enroll for the certificate
3. Enable key archival on the CA
4. Modify and enable certificate templates for key archival
Demonstration: Configuring a CA for Key Archival

In this demonstration, you will see how to configure a CA for key archival
Recovering a Lost Key

1. The private key is lost or corrupted
2. The Certificate Manager finds the serial number of the certificate
3. The Certificate Manager extracts the number PKCS#7 from the CA
4. The Certificate Manager transfers the number PKCS#7 to the KRA
5. The KRA recovers the private key
6. The user imports the private key

Serial #: 00AD036
Demonstration: Recovering a Lost Private Key

In this demonstration, you will see how to recover a lost private key.
Lab B: Deploying and Managing Certificates

• Exercise 1: Configuring Certificate Templates
• Exercise 2: Configuring Certificate Enrollment
• Exercise 3: Configuring Certificate Revocation
• Exercise 4: Configuring Key Recovery

Logon Information

Virtual machines: 20412D-LON-DC1
20412D-LON-SVR1
20412D-LON-SVR2
20412D-LON-CA1
20412D-LON-CL1

User name: Adatum\Administrator
Password: Pa$$w0rd
Estimated Time: 75 minutes
As A. Datum Corporation has expanded, its security requirements have also increased. The security department is particularly interested in enabling secure access to critical websites, and in providing additional security for features such as drive encryption, smart cards, and the Windows 7 and Windows 8 DirectAccess feature. To address these and other security requirements, A. Datum has decided to implement a PKI using the AD CS role in Windows Server 2012.

As one of the senior network administrators at A. Datum, you are responsible for implementing the AD CS deployment. You will deploy the CA hierarchy, develop the procedures and process for managing certificate templates, and deploy and revoke certificates.
Lab Review

• What is the main benefit of OCSP over CRL?
• What must you do to recover private keys?
Module Review and Takeaways

• Review Questions
• Real-world Issues and Scenarios
• Tools
• Best Practice
• Common Issues and Troubleshooting Tips