**<CHN>CHAPTER FOUR**

<CHT>ADVANCED CRYPTOGRAPHY

<COOT>Labs included in this chapter

<COOH1>

* Lab 4.1 Installing Certificate Services
* Lab 4.2 Configuring Secure Sockets Layer
* Lab 4.3 GOST Hash Function
* Lab 4.4 Configuring Certificate Auto-Enrollment
* Lab 4.5 Acceptable Encryption Policy

<COOBT>CompTIA Security+ Exam Domains

<COOBL>Domain Lab

<COOB>Threats, Attacks, and Vulnerabilities 4.2, 4.4

Technologies and Tools 4.2, 4.4, 4.5

Identity and Access Management 4.1, 4.2, 4.3, 4.4, 4.5

<COOB\_LAST>Cryptography and PKI 4.1, 4.2, 4.3, 4.4, 4.5

# **<H1>Lab 4.1 Installing Certificate Services**

**<H2>Objectives**

<TX1>Asymmetric encryption is an elegant solution to a difficult problem: how do you safely exchange symmetric keys with people all over the world using a medium (the Internet) that is so unsecure you need to use encryption in the first place? The public/private key pair allows people to share their public keys freely and use their private keys to decrypt messages and create digital signatures. Once symmetric keys are exchanged, using asymmetric encryption, the rest of the transmission is encrypted with the much faster symmetric encryption. However, at some point, human trust is required for the Public Key Infrastructure (PKI)—the hierarchy of systems that request, issue, use, and revoke digital certificates—to provide a high level of information security. Asymmetric key pairs are mathematically related so that anything encrypted by one of the keys can only be decrypted by the other key. Digital certificates are used to send public keys. But how do you know that the digital certificate you receive came from the entity that claims to have sent it? If the certificate is digitally signed by a person or an organization you trust, such as a well-known commercial certificate authority, you can assume that the certificate is legitimate. The systems that issue certificates are called certificate authorities (CA), and in this lab, you will create one.

<TX2>After completing this lab, you will be able to:

* <BL>Install a Windows Enterprise Certificate Authority
* Install a Windows 2016 Server

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Windows 10 computer with VirtualBox installed
* Windows Server 2016 ISO

**<H2>Activity**

<FE1TX1>Estimated completion time: 80–90 minutes

<TX1>In this lab, you will install an Enterprise Certificate Authority.

1. <NL\_FIRST>Open your Windows 10 desktop
2. <NL\_MID>Launch your browser and navigate to **https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2016**.
3. Click the **Sign in** button under “Windows Server 2016”
4. Enter your login credentials or create a new account.
5. Click the **Register to continue** button, and then click **Continue.**
6. Select ISO and click **Continue.**
7. Select the appropriate bit version (32 or 64) for your OS, and then select your language.
8. Click **Download.** Save the ISO to your hard drive.
9. Launch VirtualBox and create a new VM with the Windows Server 2016 ISO. Name the Virtual Machine **Windows Server,** select **Microsoft Windows** for the type, and select **Windows 2016** for the Version.
10. Start the Windows Server VM.
11. When prompted to select a start-up disk, navigate to the Windows Server 2016 ISO you downloaded. Click **Start**.
12. Click **Next**, select **Windows Server 2016 Standard Evaluation (Server with GUI)** and then click **Next**.
13. Click **Next** in the Language, Time, and Keyboard dialog box.
14. Click **Install now**.
15. Select **Windows Server 2016 Standard Evaluation (Server with GUI)** and click **Next**.
16. Accept the license terms and click **Next**.
17. Select **Custom: Install Windows only (advanced)** and accept the default setting from this point on.
18. Set the default Administrator password as **Pa$$word**.
19. Next, you need to make sure the server has Active Directory services installed. Open Server Manager, click **Manage**, then click **Add Roles and Features**. Click **Next** until you see the Server Roles window.
20. Select the Active Directory Domain Services check box and then, when prompted, click Add Features. Click Next three times. Click **Install**. This could take some time to finish.

[BEGIN NOTE]

<FE4TX1> Active Directory domain services allow the server to manage centralized settings for user accounts. You can use Active Directory to set up certificates and policies on the domain server that regulate all user accounts that have a role on the server. </FE4TX1>

[END NOTE]

1. Once the server has restarted, click the notifications flag and select **Promote this server to a domain controller**.
2. Select **Add a new forest**. Enter **Test.local** for the Root domain name. Click **Next**.
3. Enter the password **Pa$$word**, confirm it and click **Next** twice.
4. Enter **TEST** for the NetBIOS domain name and click **Next** three times.
5. Allow the prerequisites check to run. Don’t be concerned if you see warning messages, but if you receive errors, review your settings and make any necessary corrections. Once you have successfully completed the prerequisites check, click **Install**. The server will restart once it is finished.
6. Open Server Manager, click Manage, and then click Add Roles and Features. Click Next until you reach the Server Roles window.
7. Select the Active Directory Certificate Services check box, and then, when prompted, click Add Features. Click Next twice.
8. Read the Active Directory Certificate Services (AD CS) page and click Next. In the Role Services window, select the Certification Authority and Certification Authority Web Enrollment check box. If you are prompted to add features that are required for Certification Authority Web Enrollment, click Add Features. Click Next three times. In the Confirmation window, click Install.
9. Click Close after the installation has completed.
10. Click the notifications flag at the top of Server Manager, and then click Configure Active Directory Certificate Services on the destination server. Click Next in the Credentials window, and then select the Certification Authority and Certificate Authority Web Enrollment check box. Click **Next**.
11. On the Setup Type window, verify that Enterprise CA is selected and click Next. An enterprise CA uses Active Directory to authenticate users and help manage certificates. A stand-alone CA requires that an administrator approve every request for a certificate because Active Directory is not available to provide authentication. Stand-alone CAs are ideal for permitting secure network access to business partners, external consultants, or others who do not have Active Directory accounts. On the CA Type window, verify that Root CA is selected and click Next twice.
12. On the Private Key window, verify that **Create a new private key** is selected and click Next. Read the default settings on the Cryptography window and click Next.
13. On the CA Name window, in the Common name for this CA box, note the default name and click Next.
14. On the Validity Period window, accept the default settings and click Next.
15. Click Next until you reach the Server Certificate. Select **Choose and assign a certificate SSL later**. Click **Next**.
16. In the Confirmation window, click Configure, and then click Close.
17. Open a Microsoft Management Console by clicking **Start** and typing **mmc**. Select the mmc. Click **File**, the click **Add or Remove Snap-ins.** Add Certificate Templates, Certification Authority (local), Enterprise PKI, and Internet Information Services (IIS) Manager (not Internet Information Services 6.0) snap-ins, as shown in Figure 4-1. Save the console on your desktop as PKI.

<FGN>4-1</FGN>

**<FGBL>Figure 4-1 PKI console</FGLB>**

1. Close all windows and log off.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>4.3 Given a scenario, implement identity, and access management controls
* 4.4 Given a scenario, differentiate common account management practices
* 6.1 Compare and contrast basic concepts of cryptography.
* 6.4 Given a scenario, implement public key infrastructure.

**<H2>Review Questions**

1. <MULT>Which of the following roles must be available on a network to implement an Enterprise CA that supports web enrollment? (Choose all that apply.)
   1. **<MULTA>DNS server**
   2. **Active Directory Domain Services**
   3. **Certificate Services**
   4. **Web server**
2. <MULT>Which role service was not installed in this lab? (Choose all that apply.)
   1. <MULTA>Active Directory Certificate Services
   2. **Online Responder**
   3. World Wide Web Publishing Service
   4. **Network Device Enrollment Service**
3. <MULT>Which of the following statements is considered a recommended configuration or best practice for Active Directory Certificate Services? (Choose all that apply.)
   1. **<MULTA>Protect encrypted data from loss by configuring key archival and recovery for EFS certificates.**
   2. Avoid placing certificates on smart cards because loss of the smart card requires initiating the certificate revocation processes.
   3. **Enhance certificate revocation checking by setting up an online responder.**
   4. **Enhance wireless network security by requiring certificates for authentication and encryption.**
4. <MULT>The private key created in Step 32 of this lab will be duplicated on every digital signature or digital certificate issued by the CA. (**True** or False)?
5. <MULT>Which of the following statements regarding Windows Server 2016 certificate authorities is correct?
   1. <MULTA>An enterprise CA requires users to request certificates.
   2. **A stand-alone CA cannot automatically approve requests for certificates.**
   3. An enterprise CA is integrated with the NWLink service.
   4. A stand-alone CA is integrated with Active Directory Domain Services.

# **<H1>Lab 4.2 Configuring Secure Sockets Layer**

**<H2>Objectives**

<TX1>Secure Sockets Layer, now incorporated into Transport Layer Security as SSL/TLS, has been the security standard for communications between web browsers and web servers for over 10 years. The client and the server exchange public keys, use asymmetric encryption to secure their negotiations, agree on a symmetric key, and then communicate using the symmetric key thereafter. The digital certificate presented to the client by the server has been signed by a commercial certificate authority trusted by the client. The root certificates placed in the client’s certificate store by the operating system vendor determine which commercial CAs the client trusts. Of course, the client can install other certificates, but this is unusual in the e-commerce world. This is much more likely within intranets (private, corporate networks) where employees are using an in-house CA to provide certificates for encrypting email, installing on smart cards, digitally signing documents, and so forth. In this lab, you prepare the certificate authority to respond to clients’ web requests for digital certificates.

<TX2>After completing this lab, you will be able to:

* <BL>Configure a web server to support SSL connections
* Import a root certificate to a client system
* Explain how asymmetric and symmetric encryptions are used by SSL
* Configure Internet Explorer to trust a secure site

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Windows 2010 with VirtualBox installed
* Successful completion of Lab 4.1

**<H2>Activity**

<FE1TX1>Estimated completion time: 30–40 minutes

<TX1>In this lab, you prepare the server to accept web enrollment.

1. <NL\_FIRST>Launch the Windows Server VM you created in Lab 4.1.
2. <NL\_MID>Open the PKI console on your desktop. Expand Enterprise PKI in the left pane and click ServerName, it should start with the word TEST. The Enterprise PKI utility tracks the state of the CA. Any items with red markers in the center pane have problems. Figure 4-2 shows the result of a successful setup, with no red markers. Double-click CA Certificate in the center pane. Notice, on the General tab, the purposes for using this certificate. Who issued the certificate, and to whom was it issued? This is the CA’s self-signed certificate, and it represents the highest level of trust in this PKI implementation. In other words, since the CA signed its own certificate, users of any of the CA’s certificates must trust the CA; they cannot look to other entities to assure them that the CA is trustworthy. Close the certificate and examine the other items in the center pane. What is a certificate revocation list? You should not see any warning icons on these items.

<FGN>4-2</FGN>

**<FGLB>Figure 4-2 Enterprise PKI showing a healthy CA</FGLB>**

1. Expand Certification Authority (Local) in the left pane; expand and then click your server’s name. In the center pane are the certificate folders (see Figure 4-3). Explore the folders.

<FGN>4-3</FGN>

**<FGLB>Figure 4-3 Certificate folders</FGLB>**

In the Issued Certificates folder, you will find a certificate with a Request ID of 2. What certificate has the Request ID of 1, and why is it not shown in the Issued Certificates folder? Double-click the certificate with the Request ID of 2 and investigate its purpose, issuer, and so forth. Take note of the information on the Certification Path tab. This certificate has been digitally signed by the CA root. Any client or service that trusts the ServerName will trust this certificate. Click OK to close the certificate.

1. In the left pane, click Certificate Templates under Certificate Authority/ServerName. In the center pane are some of the available preconfigured certificate templates (see Figure 4-4).

<FGN>4-4</FGN>

**<FGLB>Figure 4-4 Certificate templates</FGLB>**

These certificates permit a variety of functions. You should be familiar with the EFS Recovery Agent certificate, which allows recovery of an encrypted file if the user’s key is corrupted or unavailable. Computer and User certificates are common, too. One template of note in this list is the Enrollment Agent certificate. This is required by the user who will generate certificates to be coded on smart cards. Close and save the PKI mmc.

1. Click **Start** on the server. Click Administrator Tools, double-click the Internet Information Services (IIS) Manager node and click No in the dialog box that appears. The IIS 8 Application Server Manager console appears (see Figure 4-5). In the Connections pane, expand your server’s name. Click no if the Dialog pops-up. Expand the Sites folder and expand Default Web Site.

<FGN>4-5</FGN>

**<FGLB>Figure 4-5 IIS 8 Manager </FGLB>**

1. Verify that your server’s name is selected in the left pane, and then double-click Authentication. Notice whether Anonymous Authentication is enabled. Normally, websites allow anonymous access to attract potential customers, but in a certificate service website, anonymous access would involve a serious security vulnerability. Click Default Web Site in the left panel and double-click Authentication. Here, notice the status of Anonymous Authentication. Click Default Web Site in the left pane. Scroll down and double-click SSL Settings.
2. Secure Sockets Layer provides authorization and encryption services for web-based communications. If the SSL boxes are dimmed, you need to bind HTTPS and a web server certificate to port 443, the standard HTTPS port. To set the binding, click ServerName in the left pane and, in the middle pane, scroll down and double-click Server Certificates. You should see two certificates in the middle pane. If only one certificate appears, reboot the server and then return to this console. Scroll horizontally to see more information about the certificates.
3. Double-click the top certificate and examine the three tabs, paying special attention to the purpose(s) of the certificate and the Certification Path. Click OK to close the Certificate window and double-click the other certificate. What are the purposes of the second certificate? Click OK to close the Certificate window.
4. Click Default Web Site in the left pane. In the Actions section of the right pane, click Bindings. Note that HTTP is already bound to port 80. If HTTPS is not bound, then Click Add, set Type to https (note that port is set to 443), and in the SSL certificate box, use the drop-down menu to select the certificate that is named with the fully qualified domain name of ServerName (see Figure 4-6). Click OK and click Close.

<FGN>4-6</FGN>

**<FGLB>Figure 4-6 HTTPS binding configured</FGLB>**

1. Click Default Web Site in the left panel and then scroll down and double-click SSL Settings. Now, SSL is available. Select the Require SSL check box. Click Apply in the Actions pane.
2. Create a domain user account for Anthony Newman, with the username anewman and the password Pa$$word. Double-click Anthony Newman’s account and, on the General tab, in the email box, type anewman@teamx.net and click OK. Note: you may need this account for testing purposes.
3. Close all windows and shut down the VM.

**<H2>Certification Objectives**

<TXT>Objectives for CompTIA Security+ Exam:

* <BL>1.2 Given a scenario, implement secure protocols.
* 2.3 Given a scenario, troubleshoot common security issues.
* 4.3 Given a scenario, implement identity and access management controls.
* 6.4 Given a scenario, implement public key infrastructure.

**<H2>Review Questions**

1. <MULT>The most common method of securing e-commerce transmissions is dependent on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
   1. <MULTA>the client trusting the entity that digitally signed the web server’s certificate
   2. the web server installing its root certificate in the client’s certificate store
   3. the web server installing its public key on the client using a cookie
   4. **the client and web server exchanging root certificates**
2. <MULT>The default port for HTTPS is \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
   1. <MULTA>25
   2. 80
   3. 110
   4. **443**
3. <MULT>In this lab, if SSL was initially not selectable; you could not configure SSL because \_\_\_\_\_\_\_\_\_\_\_\_.
   1. <MULTA>the CA had not yet issued an SSL certificate
   2. SSL requires greater than 128-bit encryption
   3. anonymous authentication was permitted
   4. **no port had been configured to “listen” for https requests**
4. <MULT>The purpose of enabling Active Domain Services on the server is?
   1. <MULTA>To minimize network traffic
   2. To be able to configure the web server
   3. **To have a location for centralized account maintenance**
   4. Every server should be an active domain controller.
5. <MULT>When anonymous authentication is used with IIS, the username and password traverse the network without encryption. (**True** or False)?

# **<H1>Lab 4.3 GOST Hash Function**

**<H2>Objectives**

<TXT>The GOST hash function was created by the Soviet Union. It is meant to be the standard for hash functions throughout the Soviet Union. The overall structure of GOST is very closely related to the US DES standard. GOST is an iterative function that produces a 256-bit hash value. The benefit of the iterative process is that it generates a checksum over the entire input message. The GOST function is also often referred to as a block cipher because the iterative process is done in blocks of input streams.

<TX2>After completing this lab, you will be able to:

* <BL>Analyze a hash function
* Evaluate hash functions for their strengths and weaknesses

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Windows 10
* Access to the internet

**<H2>Activity**

<FE1TX1>Estimated completion time: 20–30 minutes

In this lab, you compare and contrast different hashing algorithms.

1. <NL\_FIRST>Open Windows 10 and launch your browser.
2. <NL\_MID>Navigate to **https://www.esat.kuleuven.be/cosic/publications/article-2091.pdf**.
3. Read the article and take notes on the characteristics of the function and how it works. Don’t be concerned if you can’t understand the entire algorithm; focus on the process, especially inputs and outputs.
4. Per the article, what is a collision attack?
5. Per the article, how does GOST handle collision attacks?
6. Describe the birthday paradox referred to in the article.
7. How can the birthday paradox be used to limit the number of possibilities offered by the hash function?
8. Open another tab in your browser and navigate to **https://www.esat.kuleuven.be/cosic/publications/article-2091.pdf**.
9. Click **Download PDF** in the right panel. Read the article.
10. What similarities can you determine between GOST and DES?
11. Describe any advantages of using one over the other.
12. Why was DES created and where was it first used? Is it still in use today?

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>1.2 Compare and contrast types of attacks
* 6.1 Compare and contrast basic concepts of cryptography
* 6.2 Explain cryptography algorithms and their basic characteristics.

**<H2>Review Questions**

1. <MULT>What is the highest complexity of evaluations that can be handled by the GOST algorithm?
   1. <MULTA>2256
   2. 2128
   3. 232
   4. **296**
2. <MULT>The GOST algorithm produces a \_\_\_\_\_\_\_\_ bit hash value.
   1. <MULTA>32
   2. 64
   3. 128
   4. **256**
3. <MULT>GOST is an iterated hash function (True or False)?
4. <MULT>DES is meant to be used on what type of cipher?
   1. <MULTA>**block**
   2. streaming
   3. segmented
   4. changing
5. <MULT>It is possible that a one-way hash function maps pairs of values to the same output? (**True** of False)

# **<H1>Lab 4.4 Configuring Certificate Auto-Enrollment**

**<H2>Objectives**

<TX1>Most users do not care about digital certificates. They use them for encrypting and decrypting files and emails and digitally signing documents only when corporate security policy requires them to do so. For most users, the less they know about security details, the better; they would find the process of manually requesting certificates on a webpage an odious task. Ideally, security measures would be completely transparent to the average user. We are not there yet, but with group policies, users and their computers can be issued certificates, have them installed, and receive renewed versions when they expire without ever being aware of the process.

In Windows Server 2016, a CA administrator implements certificate auto-enrollment as follows:

1. <AL>An auto-enrollment group policy is enabled for users, computers, or both.
2. Either a custom certificate is created or a certificate template is duplicated.
3. Permissions are set on the new template to allow Read, Enroll, and Autoenroll permissions for the Active Directory security group of users or computers that require the certificate.

<TX2>After completing this lab, you will be able to:

* <BL>Configure and implement group policies for auto-enrollment of certificates
* Configure and implement certificates from certificate templates
* Explain how group policies can make the implementation of certificates transparent to users

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Windows 10 with VirtualBox installed
* Windows Server 2016 ISO
* Completion of Lab 4-2

**<H2>Activity**

<FE1TX1>Estimated completion time: 20–30 minutes

<TX1>In this lab, you implement certificate auto-enrollment through group policy, create a digital certificate from a certificate template, issue and install the template on a client, and verify the success of the procedure.

* 1. <NL\_FIRST>Launch the Windows server VM that was created in Lab 4-2.
  2. <NL\_MID>Open the PKI console on your desktop. Add the Group Policy Management snap-in. The Add or Remove Snap-ins window should now be like Figure 4-7.<FGN>4-7</FGN>

**<FGLB>Figure 4-7 Revised PKI Console</FGLB>**

* 1. Create a group policy for auto-enrollment as follows: From the PKI console, expand Group Policy Management, expand Forest: Test.local, expand Domains, expand Test.local, right-click Default Domain Policy, and click Edit. Expand User Configuration if necessary, expand Policies, expand Windows Settings, expand Security Settings, and click Public Key Policies; in the right pane, right-click Certificate Services Client – Auto-Enrollment and click Properties. On the Enrollment Policy Configuration tab, set the Configuration Model to Enabled and place check marks in the boxes to the left of Renew expired certificates, update pending certificates, and remove revoked certificates and Update certificates that use certificate templates. Your configuration should look like Figure 4-8. <FGN>4-8</FGN>

**<FGLB>Figure 4-8 Auto-enrollment group policy</FGLB>**

* 1. Click OK. Close the Group Policy Management Editor.
  2. Make a certificate template available for distribution through auto-enrollment as follows: In the PKI console, expand Certification Authority (Local), expand ServerName, and click the Certificate Templates folder. To be distributed to users and computers, a certificate must be placed in this folder. You will modify an existing certificate template and then place it in this folder.
  3. Click the Certificate Templates node under the Console Root (not the Certificate Templates folder you viewed in Step 4). Scroll down in the middle pane and right-click the User template. Click Duplicate Template. Click the General tab, then in the Template display name box, type ServerName; in the Validity period number box, change 1 to 2 years; in the Renewal period number box, change 6 to 12 weeks. In the Request Handling tab, click the radio button to the left of Prompt the user during enrollment. Notice the option to Archive subject’s encryption private key. Is this a risky setting to enable? Why or why not? Also, notice the option to Allow private key to be exported (permitting users to export their private key and remove it and place it in a safe place). Notice that the Security tab includes permissions that determine which users can request (Enroll) or have the certificate installed automatically (Enroll and Autoenroll selected). Note that none of the security principles listed in the template’s access control list has the permissions necessary to enable auto-enrollment: Allow Read, Enroll, and Autoenroll.
  4. On the **Security** tab, click the Add button; in the Enter the object names to select box, type Anthony Newman and click OK. In the Group or user names box, select Anthony Newman, and in the Permissions for Anthony Newman box, place check marks in the Allow column for Enroll and Autoenroll (leaving the default Allow Read permission enabled). Normally, it is poor administrative practice to assign permissions to individual users instead of groups, but just to demonstrate the auto-enrollment policy function in a lab environment, this user assignment is acceptable. Click OK.
  5. Return to Certification Authority (Local)/ServerName-CA and right-click Certificate Templates. Click New and click Certificate Template to Issue. In the Enable Certificate Templates window, scroll down and select ServerName and click OK. The new certificate now appears in the Certificate Templates folder (see Figure 4-9).<FGN>4-9</FGN>

**<FGLB>Figure 4-9 New Certificate Template</FGLB>**

* 1. Double-click ServerName in the middle pane and examine the purposes for which the certificate can be used. Click Cancel.
  2. Close all windows and log off the systems.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>1.2 Given a scenario, implement secure protocols.
* 2.3 Given a scenario, troubleshoot common security issues.
* 4.3 Given a scenario, implement identity and access management controls.
* 6.4 Given a scenario, implement public key infrastructure.

**<H2>Review Questions**

1. <MULT>Which of the following is considered a best practice in the handling of EFS certificates?
   1. <MULTA>Users should export their public keys and store them in a safe place.
   2. **Recovery agents should export their private keys and store them in a safe place.**
   3. Users should export their symmetric keys and store them in a safe place.
   4. EFS key pairs should always be encrypted.
2. <MULT>You are a network administrator of a Windows Server 2016 domain tasked with implementing the auto-enrollment of user certificates, which will be used to digitally sign emails. You perform the following procedures:
3. <AL>Install an enterprise root CA.
4. Choose a certificate template that allows users to digitally sign emails.
5. Duplicate the certificate template.
6. Assign permissions of Read, Enroll, and Autoenroll to the global security group that contains the users who need to be able to digitally sign emails.
7. Edit the Default Domain Policy and enable the Certificate Services Client Auto-Enrollment policy in User Configuration/Policies/Windows Settings/Security Settings/Public Key Policies.
8. Run gpupdate /force on the domain controller.
9. Log on to a domain workstation with a test domain account that is a member of the global security group to which you assigned Read, Enroll, and Autoenroll permissions to the certificate template.
10. Create an mmc that contains the Certificates snap-in.
11. Right-click the Certificates—Current User node under the Console Root, click All Tasks, and click Automatically Enroll and Retrieve Certificates.

The certificate does not appear in the user’s Certificates console. The most likely reason for this is that \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

* 1. **<MULTA>you did not issue the certificate template**
  2. you did not assign the global security group the View permission to the certificate template
  3. only administrators can manually trigger the enrollment and installation of certificates
  4. you did not run gpupdate /force on the workstation

1. <MULT>In Lab 4.4, Anthony Newman received a certificate based on the User template. Which of the following statements regarding these certificates is correct? (Choose all that apply.)
   1. **<MULTA>Both certificates allow Anthony Newman to use the Encrypting File System.**
   2. Once a User certificate is issued to a user, the best practice is to revoke the user’s EFS certificate.
   3. The User certificate contains three different private keys, one for each of the three purposes of the certificate.
   4. **Both certificates were issued by *ServerName*.**
2. <MULT>In this lab, the auto-enrollment policy was configured so that all domain users could receive the certificate based on the User certificate template. (True or **False**)?
3. <MULT>Anthony used the certificate he received in Lab 4.4 to place his digital signature on an email to a customer named Helene Grimaud. For Helene to be sure that the email came from Anthony, she must \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
   1. **<MULTA>trust ServerName**
   2. install Anthony’s certificate
   3. compare the thumbprint on Anthony’s certificate with the result of her own hashing of his certificate
   4. send Anthony her certificate

# **<H1>Lab 4.5 Acceptable Encryption Policy**

**<H2>Objectives**

<TX1>An Acceptable Encryption Policy is instituted by organizations that wish to detail how encryption protocols will be handled within the organization. Such a policy is essential in understanding what type of encryption will be used for data. An Acceptable Encryption Policy specifies what cryptographic hash(es) should be used to secure data.

<TX2>After completing this lab, you will be able to:

* <BL>Define an Acceptable Encryption Policy
* Identify the different types of encryption protocols
* Identify different types of hash algorithms for encryption

**<H2>Materials Required**

<TXT1>This lab requires the following:

* <BL>A computer with Internet access

**<H2>Activity**

<FE1TX1>Estimated completion time: 30–40 minutes

* 1. <NL\_FIRST>Open your web browser and go to http://www.sans.org/security-resources/policies/.
  2. <NL\_MID>Click General, then Click Acceptable Encryption Policy.
  3. Download the DOC version of the template.
  4. Replace <Company Name> throughout the document with *Your\_Last\_Name* Securities. For example, if your last name is “Smith,” then the company name should be “Smith Securities.”
  5. In Section 4.1.3 of the document, notice the three different types of encryption algorithms. Identify a fourth type of encryption algorithm and add it to the table.
  6. Click the link for RFC6090 in the table and read the memo associated with the algorithm. Do the same for PKCS#7 padding scheme and the LDWM Hash-based Signatures Draft.
  7. In Section 4.2, click the link for NIST Policy on Hash Functions. Explore the website and determine what hash functions are for and why they are important.
  8. Remove the revision history from the end of the template and add your own revision history.
  9. If desired, save the file with a naming convention provided to you by your instructor.
  10. Make sure you read through the policy once you have completed it. Identify all the key components of the policy.
  11. In which section of the company’s Computer Security Policy does this policy belong?
  12. What is an appropriate review cycle for this certificate?

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>2.3 Given a scenario, troubleshoot common security issues
* 4.4 Given a scenario, differentiate common account management practices.
* 6.1 Compare and contrast basic concepts of cryptography.
* 6.4 Given a scenario, implement public key infrastructure

**<H2>Review Questions**

1. <MULT>The Infosec team referred to in the document is the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ team.
   1. <MULTA>Information technology
   2. General committee of security
   3. **Information Security**
   4. Help Desk support
2. <MULT>NIST stands for:
   1. <MULTA>National Institute of Security Technology
   2. **National Institute of Standards and Technology**
   3. National Institute of Secondary Teachers
   4. None of the above
3. <MULT>You should not follow national standards when creating cryptographic protocols, because people know those policies and they are easy to decode. (True or **False**)?
4. <MULT>When implementing a padding scheme, you must first encrypt the data and then pad the encryption. (True or **False**)?
5. <MULT>Cryptographic keys must be generated and stored in a secure manner that prevents: (Choose all that apply.)
   1. **<MULTA>Loss**
   2. **Theft**
   3. **Compromise**
   4. **Padding**