Chapter 9: SSL and Certificate Services

The most widespread concern with the Internet is not the limited amount of bandwidth or the occasional objectionable content, but the imperative need for security when transferring data. The most common implementation of security on the Internet today is the use of digital certificates. Digital certificates can guarantee the identity of a client or server across an untrusted network and also can encrypt data. This chapter discusses the technology behind security as well as tools provided by Microsoft for ensuring Internet security.

This chapter covers the following topics:

- Secure Sockets Layer (SSL) and why it is fundamental to security
- Encryption and its role with both clients and servers
- A description of and recommendations for client certificate mapping
- Certificates and certificate authorities on the Internet
- A complete walk-though of the installation of Microsoft Certification Authority Server

An Overview of the Secure Sockets Layer (SSL)

Internet Information Services 5 provides a high-performance implementation of Secure Sockets Layer (SSL) 3.0 for secure communication and authentication with X.509 certificates, RSA Public Key Cipher, and a broad array of additional security features. SSL enables a client communicating with a server to negotiate security and authentication levels. When a session is initiated, SSL requires a symmetric session key and encryption algorithm to be negotiated. The symmetric key is used for encrypting and decrypting data. Authentication of the client/server might also be performed while the session is being established. When the negotiation is completed, the client and the server can transmit data to each other in a secure manner by encrypting the data.

Encrypting Communication

Encryption, or *cipher*, is the means of scrambling data to ensure that it cannot be easily read by unintended recipients. The encryption features offered in Internet Information Services 5 are similar to those in Internet Information Server 4, with two exceptions: The server certificate is now bound to individual Web sites, and a new wizard helps make configuring server certificates much easier.

Configuring SSL encryption in Internet Information Services 5 is pretty much the same as in Internet Information Server 4, with one exception: You now have the capability to use Server-Gated Cryptography (SGC) certificates and encryption. SGC is available for use on banking industry sites and allows these institutions to use 128-bit encryption in export versions of Internet Information Services.

Encrypting communication between a client and a server requires configuration of both. The client, or Web browser, can support 40-bit or 128-bit encryption, or both. The server is capable of encrypting

communication only after a server certificate is installed.

128-bit and 40-bit Clients

Like Microsoft Internet Explorer 5.0, Internet browsers support two encryption levels: 40-bit encryption and 128-bit encryption. 40-bit encryption is the weaker of the two; it is the maximum encryption level available for export to countries outside Canada and the United States because the U.S. government considers stronger encryption levels a threat to national security. 128-bit encryption is supported in North American versions of Internet Information Services, Internet Explorer, and Netscape Navigator.

To determine which level of encryption is installed in Internet Explorer, click the Help menu and then click the **About Internet Explorer** option. For example, in my copy of Internet Explorer 5.0, the About box lists 128-bit as the Cipher Strength.

Encryption versus Authentication

Although encryption and authentication are usually discussed together, they are two distinct topics. Authentication is the means of validating the identity of the person or processes involved in communication. Authentication can be one-way, where either party is sure about the identity of the other, or two-way, where both parties are sure of the identity of the other. Authentication with Internet Information Services 5 is covered in detail in Chapter 3, "Integrating IIS with Windows 2000 Security," and Chapter 4, "IIS Security."

Using Server Certificates

A *server certificate* is an electronic ID for your server that enables your server to perform two vital functions for secure communications: to verify its identity to users and to encrypt information going to those users. SSL encryption requires that a server certificate be bound to or associated with your Web site. This certificate contains "keys" used in forming a secure connection between your Web site and users requesting secure information.

In Internet Information Server 4, server certificates were actually bound to the Web service, not to individual Web sites, unless a Web site had a unique IP address. In Internet Information Services 5, you can bind server certificates to any Web site you want, but only one certificate per site. Also, in Internet Information Server 4, you needed to use Key Manager to bind certificates. In Internet Information Services 5, you can use the Web Site Certificate Wizard, which makes this whole process a great deal easier. The wizard guides you through the process of requesting and installing a certificate.

Client Certificate Mapping

Client certificates are the user equivalent of server certificates. A *client certificate* is a digital ID that enables a user to verify his identity to your Web server and to allow your server to use client certificate mapping. Client certificate mapping maps a client certificate to a Windows user account

and automatically authenticates and allows access to users with these certificates and the proper account.

For example, if a user named Vicky has a client certificate and clicks on a link to the company Web site's Employee Information section, her Web browser sends her certificate in the request header to the server, and the server searches for a mapping for this certificate. If the user's certificate is the correct certificate and is mapped to a valid Windows user account with permissions to the content on the site, then Vicky is automatically authenticated and the requested data appears in her browser.

Types of Certificate Mapping

Two kinds of certificate mapping exist in Internet Information Services 5: one-to-one and many-to-one. *One-to-one mapping* associates a particular certificate with a particular Windows user account. An exact copy of the client certificate must reside on the server used for authentication. If the user gets another client certificate using the exact same request, the mapping will need to be remade.

Many-to-one mapping uses only certain information in the certificate and compares it against criteria to map with user accounts. As long as a certificate is used that matches these criteria, the mapping will succeed. In this way, any number of certificates can be used to map to a single user account, thus the "many-to-one" name. Copies of the certificates do not need to reside on the server.

The difference can be clarified by using some anthropomorphisms. When a request with a certificate comes in, the server has two ways of mapping it. It can say, "I'm looking for the certificate issued to Vicky on March 3, 1999, serial number ZXV345T4689AS234, and if I don't get*that* certificate, I'm sending a "403—Forbidden" error and the deal is off." Or, the server could say, "I'm looking for*any* certificate issued by the XYZ Certificate company, issued to the ABC Corporation, between March 1, 1999, and June 1, 1999. If I get *any* certificate like that, everything is cool." The first is one-to-one mapping, and the latter is many-to-one mapping.

It is easy to see that one-to-one mapping is inherently more secure, but it requires more administrative work to set up and maintain. On the other hand, many-to-one is inherently less secure, but offers greater flexibility and requires less administrative effort.

Fortezza Cards and Certificate Mapping

Smart cards make a copy of the certificate on the card and use it for mapping. After the procedure for copying the certificate is done, the certificate can be used just like any other client certificate for mapping. Typically, one-to-one mapping is used for Fortezza cards because they were designed for higher-security situations. For more information on Fortezza cards, refer to Chapter 4.

Basic Authentication with SSL

SSL encryption can be combined with basic authentication to enhance security. SSL is most often configured to encrypt data transferred to and from the Web service—for example, to encrypt a user's credit card number when making an online purchase. When SSL is combined with basic authentication, however, the user account and password are also encrypted, making this combination of security both effective and secure.

Basic authentication with SSL security is exceptionally advantageous when used for a client with a

non-Microsoft browser. Clients with non-Microsoft browsers can now be authenticated by Internet Information Services and not have their username and password transferred in clear text across theInternet.

Digital Certificates

Internet Information Services also supports X.509 digital certificates for access control. These digital certificates must be issued by a trusted certificate authority and must be maintained on the client computer. They are similar in functionality to an ID card—that is, the client presents a digital certificate when attempting to access a resource on a Web server. However, these have one more level of security than a simple ID card. When the digital certificate is generated, the user must sign it with a password. Then, each time the certificate is used, the client must again enter the password to verify that the client is the actual owner of the digital certificate.

Use of digital certificates requires an appropriate protocol, such as SSL, on both the client and the server. Most often, servers present certificates to clients that authenticate the identity of the server or domain name. However, Internet Information Services can be configured to require a client to validate its identity with a client certificate.

Selecting Your Mapping Method

Which of the two mapping methods you use depends upon several factors, but the two major ones are the security level needed and the administrative resources available. If you need air-tight security and authentication, one-to-one mapping can't be beat, as long as you have the resources to handle it. If you have limited administrative resources and a large number of clients to map, then many-to-one works nicely, as long as very tight security is not needed. Following are several scenarios and recommendations for the appropriate mapping method to choose:

- **Small network with semi-secure information; authentication not needed.** Even though the network is small, many-to-one is still the way to go because the information is only semi-secure. You can create a single certificate and share it using a floppy disk.

- **Small network with semi-secure information; authentication needed.** If you want to know who is accessing what, you can use many-to-one mapping with one of the criteria being username, and map to individual user accounts. This is more work but is still better than one-to-one because users can get replacement certificates, and mappings do not need to be redone.

- **Small network with secure information; authentication needed.** In this case, it's best to go with one-to-one mapping and map certificates to individual accounts. This means that every time a user gets a replacement certificate, a new mapping will have to be made. But we're talking a small number of users. Or, you could take advantage of the Active Directory certificate features in Windows 2000. For more information about this, see the Windows 2000 documentation.

- **Large network with semi-secure information; authentication not needed.** The solution here is the same as for a small network, but you can use a different certificate for each department or group.

- **Large network with secure information; authentication needed.** For secure information, the

only mapping that makes sense is one-to-one, especially if you want to enforce data responsibility. However, you may choose to go with many-to-one for its simplicity of administration. Basically, it's your call here. If you go with one-to-one, use the Active Directory to lower administration overhead.

- **James Bond.** If you want the coolest way to secure information, then one-to-one mapping with Fortezza smart cards is your aim. You can use this method to enforce policies and to secure data like nobody's business. You just suavely slide your smart card through the reader, and you're in. However, if you have large numbers of clients or you turn over clients a lot, this can be an administrative nightmare.

Server Certificates and Certificate Authorities

To activate the SSL security features of Internet Information Services, you must obtain and install a valid *server certificate*. Server certificates are digital identifications containing information about your Web server, the organization validating the server's Web content, and the fully qualified domain name (FQDN) of your site. Functioning in the same way as conventional forms of identification, a server certificate enables users to authenticate your server, check the validity of Web content, and establish a secure connection.

A digital certificate is assigned to a host by using the FQDN. Because of this, certificates are totally free of any IP address constraints. You can change the IP address of the host without any effect on the certificate. For example, if you have a certificate for the Web site `http://www.company.com`, it does not matter whether that domain name is referenced to the IP address `192.168.110.123` or to the IP address `123.110.168.192`, or whether the IP address of the Web site changes after the certificate is issued and installed.

The success of a server certificate as a means of identification depends on whether the user trusts the validity of information contained in the certificate. For this reason, certificates are usually issued and endorsed by a mutually trusted, third-party organization, called a *Certificate Authority (CA)*. The CA's primary responsibility is confirming the identity of the organization registering a certificate. This ensures the validity of the identification information contained in the certificate.

To do this, a CA must have a *CA certificate*. The CA certificate identifies the CA that issued a server certificate, thus validating the server certificate. Of course, in this hierarchy, as in all hierarchies, there is a top. So, who validates the CA's certificate? At the very top, a CA must sign its own certificate because, by definition, there is no higher CA in the hierarchy. A self-signed CA is called a *root certificate*. Root certificates are text files with a `.crt` extension.

Alternatively, an organization can issue its own server certificates without a CA to sign them. For example, in the case of a large corporate intranet handling employee payroll and benefits information, the corporation could maintain a certificate server and assume responsibility for validating the identity of registrants and issuing server certificates.

Authentication Servers

To authenticate a server with a certificate issued by a particular CA, a client needs to verify that the issuing CA is listed in its Web browser's list of trusted CAs. The most common CA root certificates

are already installed in most Web browsers.

To view the CAs that are trusted by Microsoft Internet Explorer 5, perform these steps:

1. Open Microsoft Internet Explorer 5.
2. From the Tools menu, click **Internet Options**.
3. Click the **Content** tab.
4. Click the **Authorities** button in the Certificates box.

The three tabs on the Certificate Manager dialog box contain lists of all certificates known to this copy of Internet Explorer.

Each certificate contains information about the subject and issuer of the certificate, its effective or beginning date, its expiration date, and the encoded fingerprint that identifies the certificate to other clients and servers.

To review information contained in a digital certificate, select a certificate and then click the **View Certificate** button.

To add a new CA to the list of trusted authorities for your Web server, you must explicitly add the CA's certificate, called a *root* certificate, to your Web server. You can use Microsoft Internet Explorer version 4.0 or later and a command-line utility called `Iisca.exe` to add new root certificates to your server.

Certificate Wildcard Mapping

Wildcard certificates allow multiple hosts within the same domain or subdomain to use the same digital certificate. For example, with wildcard mapping, a certificate is issued to `*.domain.com`, or simply `domain.com`, but is used to support the Web sites `http://www.domain.com` and `http://www2.domain.com`. Recall that normally a certificate is issued to one specific host, such as `http://www.domain.com`.

The benefit of certificate wildcard mapping is that you need to purchase only one certificate for use on multiple Web sites, making this a very cost-effective and desirable method of securing a Web site. But not all third-party CAs allow you to request a certificate that can be used on multiple hosts. Such a certificate has a common name, such as `*.domain.com` or `domain.com`. Not all Web browsers or Web servers support their use.

When a Netscape client checks the host name in this certificate, it uses a shell expansion procedure to see if it matches. In the example given, any host ending in `domain.com` should work. However, Internet Explorer does not implement wildcard certificate name checking, so Internet Explorer clients will receive a warning saying that the host name does not match that given in the certificate. In some cases, wildcards actually work with Internet Explorer 4.0 and higher, but Microsoft states officially that Internet Explorer does not work with wildcards, so there is no guarantee that wildcarding will work with any Microsoft product for any period of time.

Distributing Certificates

An organization that has determined it needs to provide certificates to clients or vendors has three general options. First, it could create its own in-house CA that meets its own security and availability requirements. Second, it could outsource its CA requirements to a third party, such as VeriSign or Thawte. Third, it could establish a chained CA with a third-party CA that allows the organization to issue certificates to end users but leverage the established security of the third-party CA.

For example, a manufacturer might decide to issue certificates to its employees across offices in three states, or a consulting firm might issue certificates to its vendors to control access to the company extranet. The organization in this example may select and purchase secure key management hardware from leading vendors, such as BBN (GTE), Chrysalis, and Atalla, or select and purchase Certificate Authority software from vendors, such as Microsoft, Xcert, or Nortel Entrust. These technologies allow the organization to issue certificates containing custom information at a security level tailored for that organization.

Unfortunately, however, most browsers will not initially recognize those certificates. Every browser that will be verifying the trustworthiness of certificates issued by that internal CA will need to be modified to acknowledge the root key used by that organization when signing the certificates. That means that every copy of Microsoft Internet Explorer, Microsoft Outlook, and Netscape Communicator needs to have the root key for the organizational CA added before data signed by these certificates will be trusted. In a small, controlled environment, that is no problem. But in a heterogeneous, multiplatform scenario such as the Internet, it is impossible.

A chained certificate program allows a third-party CA to transfer all the trust associated with the third-party CA to the organizational CA. All the software that trusts digital certificates provided by the third-party CA will immediately begin to trust the certificates issued by that chained CA.

Installing and Configuring Certificate Services

Certification Authority Server is an add-on to Windows 2000 Server that is bundled on your Windows 2000 Server installation disk. It enables you to create a customizable service for issuing and managing X509 version 3 digital certificates for authentication purposes. You can create server certificates for the Internet or for corporate intranets, giving your organization complete control over its own certificate management policies.

A wizard is included to configure the installation. Be prepared, though: You'll need to provide accurate information at the time of installation. Review the information required before attempting an installation of Certificate Services.

To install the Certification Authority Server add-on using general configuration options, use the following procedure:

1. Place the Windows 2000 Server CD-ROM into your CD drive and then select **Install Add-on Components**.

2. The Windows Components Wizard will then prompt you to select or deselect the components

needed for your system. Click the check box for Certificate Services. You will be prompted immediately with a dialog box notifying you that once certificate services have been installed, the computer cannot be renamed and cannot join or be removed from a domain.

You should address some considerations before selecting YES to continue:

- Because you will not be able to change the computer name without a reinstall of the Windows 2000 once Certification Authority has been installed, be sure that you are comfortable with the current naming convention employed on your network, or implement a new naming convention before proceeding.
- Because you will not be able to join the computer to a domain or remove it from a domain once Certification Authority has been installed, you will need to be sure that you are comfortable with the current naming convention of the domain or subdomain on your network, or implement a new naming convention before proceeding.
- Verify that the computer is joined to the appropriate domain before proceeding.

3. Next, select the Certification Authority type in the Windows Components Wizard. There are four types:
   - Enterprise root CA
   - Enterprise subordinate CA
   - Stand-alone root CA
   - Stand-alone subordinate CA

The first CA on a network must be a root CA. To create an Enterprise CA, Active Directory must be enabled. A Stand-alone CA does not require Active Directory. Select Stand-alone root CA to implement certificate services on your intranet. See Figure 9.1.

Figure 9.1
The Certificate Authority type defines not only how Certificate Services functions on you server, but also how you will need to manage it.

4. Select CA Identifying Information in the Windows Components Wizard. Enter the appropriate data and then continue with the install. See Figure 9.2.

5. Select the Data Storage Location in the Windows Components Wizard. I recommend that the default locations be utilized. Click Next to continue.

6. Click Yes to continue if you have Internet Information Services installed and running on your computer. Microsoft Certificate Services will inform you with a dialog box that Internet Information Services must be stopped before the install can proceed.

   The Windows Components Wizard will now configure components and copy the file on your machine. An installation progress bar is provided to monitor the installation process.

7. Click Finish when the Windows Component Wizard prompts you that it has completed the configuration of the components you selected.

This chapter provided a high-level discussion of certificate services in Windows 2000 because the topic is commonly misunderstood and not frequently implemented. The next chapter discusses a more common topic: SMTP and NNTP services.

Figure 9.2
Before attempting to install Certificate Services, be sure you have all information required.