Entering a secure site

This site has a valid certificate.

This certificate is a statement guaranteeing the security of this Web site. A certificate contains information that a specific Web site is authentic. This ensures that no other site can assume the identity of the original site.

When you enter a secure Web site, Internet Explorer displays this dialog box to notify you that you are entering a secure Web site, and displays a lock icon in a locked position on the status bar. When you leave a secure Web site, Internet Explorer displays another dialog box to notify you that you are no longer on a secure Web site, and displays a lock icon in an unlocked position on the status bar.

To view the certificate for this Web site, click the **View Certificates** button in the dialog box.

If you want to see this dialog box whenever you have entered a secure Web site, make sure the **In the future, do not show this warning** check box is clear.

Entering a secure site with an invalid certificate

The certificate for this site is not valid.

A certificate contains information that a specific Web site is genuine and secure. This ensures that no other Web site can assume the identity of the original Web site. Certificates are also dated when they are issued. When you try to connect to a secure Web site, Internet Explorer verifies the information in the certificate and that the current date precedes the expiration date. If the information is not current and valid, Internet Explorer can display a warning.

To view details about the certificate, click the **View Certificate** button in the dialog box.

When you enter a secure Web site, Internet Explorer displays a lock icon in a locked position on the status bar. When you leave a secure Web site, Internet Explorer displays a dialog box to notify you that you are no longer on a secure Web site, and displays a lock icon in an unlocked position on the status bar.

File Download

Some files can contain viruses or otherwise harm your computer.

If you run this program or open this file now, and it causes your computer or other programs to shut down, you could lose unsaved work in any open files on your computer.

If you save this file or program to disk, you can run it later. This would allow you to take precautions such as the following before you open the file or run the program:

- Check the file with a virus scanner.
- Save your work and close other programs.
- Disconnect from the Internet or any other network connections.

For the most security, make sure the **Always ask before opening** check box is selected. If you feel confident that this type of file or program is always safe to open or run directly from the Internet, make sure this check box is clear.

Sending and Receiving Information About Your Browsing

Some Web sites create files on your computer to save information about your identity and preferences when visiting that Web site. These files, often called "cookies," can store only the information you provide. In other words, when these files are created, you will be asked before any personal information—such as your name, e-mail name, account names, and password—is stored. These files cannot store personal information or retrieve new information from your computer without your permission.

After this file is created for a Web site, information from your computer is sent to that Web site whenever you visit it, so that the content and options for the Web pages are tailored to you.

These files are usually stored in your Windows folder—for example, C:\Windows\Cookies. If you look in that folder, you will find that these files are small, usually less than 2K each. You cannot edit or view these files yourself—they do not record information in plain text.

If you frequently visit Web sites that request sending and receiving this information, and you feel safe storing this information on your computer, make sure the **In the future, do no show this warning** check box is selected.

Signed Program Download

The certificate for this program is valid.

A certificate contains information that a specific software program is genuine. This ensures that no other program can assume the identity of the original program. Certificates are also dated when they are issued. When you try to download software, Internet Explorer verifies the information in the certificate and that the current date precedes the expiration date. If the information is not current and valid at the time of download, Internet Explorer can display a warning.

This program's publisher has obtained a certificate for this program, from a recognized certificate issuer, so that the authenticity of this program can be verified.

Any software or component you install can potentially harm your computer.

To view details about the software, click the underlined program name in the dialog box. If the program name is not underlined, the publisher did not furnish a WWW address to obtain additional information.

To view details about the certificate, click the underlined software publisher's name in the dialog box.

Given what you know about this software, its publisher, and your computer, you must decide whether to proceed with installing and running this software. Additionally, if you trust this software publisher completely, you can choose to bypass this dialog box in the future for all software from this publisher that has certificates, and automatically install and run their software.

If, given this information, you still do not feel confident in installing this software, then click **No**.

Signed and Invalid Program Download

The certificate for this program is **not** valid.

A certificate contains information that a specific software program is genuine. This ensures that no other program can assume the identity of the original program. Certificates are also dated when they are issued. When you try to download software, Internet Explorer verifies the information in the certificate and that the current date precedes the expiration date. If the information is not current and valid, Internet Explorer can display a warning.

This program has a certificate but it cannot be verified.

Any software or component you install can potentially harm your computer. Or, the software or component may be unstable.

To view details about the software, click the underlined program name in the dialog box. If the program name is not underlined, the publisher did not furnish a WWW address to obtain additional information.

To view details about the certificate, click the underlined software publisher's name in the dialog box.

Given what you know about this software, its publisher, and your computer, you must decide whether to proceed with installing and running this software.

If, given this information, you still do not feel confident about installing this software, then click **No**.

Signed and Invalid Web site

The certificate for this Web site is not valid.

A certificate contains information that a specific software program is genuine. This ensures that no other program can assume the identity of the original program. Certificates are also dated when they are issued. When you try to download software, Internet Explorer verifies the information in the certificate and that the current date precedes the expiration date. If the information is not current and valid, Internet Explorer can display a warning.

This program has a certificate but it cannot be verified.

Any software or component you install can potentially harm your computer. Or, the software or component may be unstable.

To view additional details, click the **View Details** button in the dialog box.

Given what you know about this Web site, its publisher, and your computer, you must decide whether to proceed with entering this Web site.

If, given this information, you still do not feel confident about installing this software, then click **No**.

Unsigned Program Download

This software does not have a certificate, so it might not be safe to install and run on your computer.

A certificate contains information that a specific software program is genuine. This ensures that no other program can assume the identity of the original program.

The software publisher has not obtained a certificate for this software from a recognized certificate issuer, so the authenticity of this software cannot be verified.

Given what you know about this software, its publisher, and your computer, you must decide whether to proceed with installing and running this software.

If, given this information, you still do not feel confident about installing this software, then click **No**.

Insecure content download from a secure Web site

The Web site you are viewing is a secure Web site. It uses a security protocol such as SSL (Secure Sockets Layer), or PCT (Private Communications Technology), to secure information you send and receive.

However, this Web page contains items from other Web sites which are not secure.

Given what you know about this Web site, and your computer, you must decide whether to proceed with downloading the insecure items.

If, given this information, you still do not feel confident about installing this software, then click **No**.

Entering a non-secure Web site from a secure Web site

The Web site you were viewing was a secure Web site. It uses a security protocol such as SSL (Secure Sockets Layer), or PCT (Private Communications Technology), to secure information you send and receive.

However, the Web page you are entering does not have a certificate and is not secure.

Given what you know about this Web site, and your computer, you must decide whether to proceed with entering this Web site.

If, given this information, you still do not feel confident about entering this Web site, then click **No**.

Remove

To remove an item from the list, first click on the name and then on **Remove**.

List of Trusted Publishers and Credentials Agencies

This list controls whose software can be installed on your system without asking you first.

The list can contain both individual software publishers and commercial software publishers. Software that has been published by a publisher in this list can be installed without your explicit approval.

The list can also contain one or more credentials agencies. Similar to a notary, a credentials agency is an organization in the business of attesting to the identity of software publishers. If a credentials agency is in this list, then *any* publisher certified by that agency is considered trusted, allowing software they publish to be installed on your system without asking you first.

Consider All Commercial Software Publishers Trustworthy

A commercial software publisher is a bona fide company in the business of producing or selling computer software. In addition, commercial software publishers have met certain minimum financial criteria that attest to their ability to support their software on a continuing basis.

Checking this box means that software that is correctly signed by *any* commercial software publisher can be installed on your system without first asking for your approval.

Digital Signatures

Digital signatures are similar to handwritten signatures. When you sign a document, you are taking responsibility for it. Digital signatures do the same thing. The most trustworthy signatures carry a legally binding certificate verifying that the signer is who he or she claims to be.

Digital signatures are relatively new and not everyone uses them. Many pieces of software do not yet carry a signature.

Certificates

A certificate is a guarantee that a digital signature is valid. Certificates are issued by various organizations. These organizations are similar to notaries and certificates are similar to the seals notaries place on documents, certifying that the signers are who they say they are.

Description of Content

This field should be the description of the content which is being digitally signed. It should be kept simple and concise, less than one line.

URL to Receive More Information

This field can be any standard URL for the recipient to go to get more information on the content that is being digitally signed. (e.g.: http://www.mysite.com/mycontent or mailto: me@mysite.com)

Timestamp Server Address

This is the HTTP URL address of a server that issues digital time stamps using Microsoft's Timestamp Requester. Currently, Verisigns' is the most popular (http://timestamp.verisign.com/scripts/timstamp.dll). If this field is left blank, the signature on your content will expire the same time your signing certificate expires.

Remove this help ID

Displays the name of the person or company to which the certificate was issued.

Displays the name of the Certification Authority who issued the certificate.

A Certification Authority (CA) is an entity entrusted to issue certificates asserting that an individual (or organization) requesting the certificate fulfills the conditions of an established policy.

Click this to install the certificate into one of the certificate stores.

Click this to modify editable certificate properties, such as friendly name and description, or further restrict the list of allowed purposes.

Click this to view more information about the issuing Certification Authority, if available.

Click this to accept the certificate.

Click this to decline the certificate.

Displays a list of purposes for which the Certification Authority intended the certificate to be used.

Remove this help ID

Displays the time period for which the certificate is valid.

Displays whether you have a private key associated with the certificate.

A private key is the secret half of a key pair used in public key security. Private keys are used to digitally sign messages or decrypt messages that have been encrypted with the corresponding public key.

Displays the current the list of X.509 fields or extensions shown below. You can select to view a section of the list.

Click this to save a copy of the certificate to a file.

Displays the list of all X.509 fields, extensions and associated properties found in the certificate.

 represents a X.509 Version 1 field.

 represents a non-critical X.509 Version 3 extension.

 represents a critical X.509 Version 3 extension.

 represents an editable property that is associated with the certificate.

Displays the selected field or extension in detail.

Displays the certification path for this certificate. A certification path is a chain of related certificates.

Displays the selected certificate or certificate trust list in detail.

Displays the status of the selected certificate or certificate trust list.

Displays the list of attributes and associated properties in the certificate trust list.

 represents an attribute in the certificate trust list.

 represents a non-critical extension.

 represents a critical extension.

 represents an editable property that is associated with the certificate trust list.

Displays the selected attribute or extension in detail.

Click this to view the digital signature of the certificate trust list.

Displays the list of certificates contained within the certificate trust list.

Displays the selected certificate in detail.

Displays the selected X.509 field or extension in detail.

Displays the selected certificate.

Displays the list of attributes and associated properties in the certificate revocation list.

 represents an attribute in the certificate revocation list.

 represents a non-critical extension.

 represents a critical extension.

 represents an editable property that is associated with the certificate revocation list.

Displays the selected attribute or extension in detail.

Displays the list of revoked certificates contained within the certificate revocation list.

Displays the selected certificate in detail.

Displays the selected attribute or extension in detail.

Displays the friendly name that is associated with the certificate.

Displays the description that is associated with the certificate.

Displays the list of purposes that the Certification Authority intended for certificate.

Click this to add a certificate purpose that is not listed.

Click this to add a certificate purpose that is not listed.

Click this to add a certificate purpose that is not listed.

Click this to add a certificate purpose that is not listed.

Displays the name of the signer.

Displays the email address of the signer.

Displays the date and time when the file was signed.

Displays the certificate referenced by the signature.

Displays a list of all countersignatures.

Displays more information about the selected countersignature.

Displays a list of all attributes in the signature.

Displays the selected attribute in detail.

Click this to select the certificate store.

Click this to close the dialog without making a selection.

Displays all the certificate stores that are available for selection.

Displays the certificate store hierarchy so that components of a logical store (called physical stores) are also available for selection.

Click this to select the certificate.

Click this to close the dialog without making a selection.

Click this to see more details about the certificate.

Displays a list of certificates available for selection.

Displays a list of certificates in the system according to the tab and purpose selected.

Displays only the certificates that have the selected certificate purpose.

Click this to import a certificate from a file on disk.

Click this to export the selected certificate(s) to a file.

Click this to see more details about the selected certificate.

Click this to remove the selected certificate(s) from the system.

Click this to set advanced options.

Click this to close the dialog box.

Displays the name of the person or company to which the certificate was issued.

Displays the name of the Certification Authority who issued the certificate.

Displays the expiration date of the certificate.

Displays the intended purpose(s) of the certificate.

Displays the friendly name associated with the certificate.

Displays the name of the person or company to which the certificate was issued.

Displays the name of the Certification Authority who issued the certificate.

Displays the expiration date of the certificate.

Displays the intended purpose(s) of the certificate.

Displays the friendly name associated with the certificate.

Displays a list of all known certificate purposes. You can designate any purpose as “advanced” by selecting its checkbox.

Displays the default file format used when you export certificates by dragging them to a file folder. **DER Encoded Binary X.509** is a binary format suitable for exporting a single certificate. **Base64 Encoded X.509** is a textual representation of a DER-encoded certificate useful when sending a certificate to a non-Windows computer. You may export all certificates in a certification path using a **PKCS #7** format file.

Specifies whether to include the certificates in the certification path when exporting using drag and drop. This checkbox is only available when you use **PKCS #7** format files for export as only **PKCS #7** supports multiple certificates in a single file.

Closes the dialog box without saving any changes you have made.

Click this to select a Certification Authority.

Click this to close the dialog without making a selection.

Displays a list of Certification Authorities published in the Active Directory.

Closes the dialog box and saves any changes you have made.

Displays a list of signatures.

Displays the selected signature in detail.