Certify your

Software Integrity

with thawte Code Signing Certificates

Sign your code and active content for secure online distribution...

thawte
it's a trust thing

1. Overview

As a software developer you know that the product you make available on the Internet can be tampered with (without detection) if it is not secured. You want customers to know that the software really comes from the publisher who signed it and that it has not been altered or corrupted. That is why you need a Code Signing Certificate from *thawte*.

thawte is dedicated to making the Internet a secure and viable platform for commerce and the distribution of content. A *thawte* Code Signing Certificate ensures customers downloading your software from the Internet that the code has not been tampered with. With a *thawte* Code Signing Certificate, your code will be as safe and trustworthy as it would be if you shrink-wrapped it and sold it off a store shelf.

This guide will show you how Code Signing Certificates are used to secure code that can be downloaded from the Internet. You will also learn how these certificates operate with different software platforms.

2. Why a *thawte* Code Signing Certificate?

Customers trust software they buy in a store because they can tell who published the product and can see whether the package has been opened or not.

The Internet cannot offer the reassurance provided by shrink-wrapped software. When customers download software from the Internet, the most they see is a message warning them about

As a solution major software vendors such as Netscape and Microsoft have developed tools for code signing. Code signing allows a developer to sign his/her application digitally. On the strength of that signature, the browser or operating system then decides whether or not to trust the software.

When customers download software signed with a *thawte* Code Signing Certificate, they can be assured of:

Content source:
: The software really comes from the publisher who signed it.

Content integrity:
: The software has not been altered or corrupted since it was signed.

A *thawte* Code Signing Certificate goes a long way in establishing user confidence.

Users have recourse to the publisher, should the software perform a malicious or unacceptable activity on their computers. This accountability and possibility of recourse serve as a strong deterrent to the distribution of harmful code.

Developers and webmasters benefit from signed code because it positively supports their reputation and makes their products harder to falsify. By signing code, developers build a relationship of trust with users. Users will gain confidence in downloading signed software from that publisher or web site.

3. Who needs a Thawte Code Signing Certificate?

Any publisher who plans to distribute code or content over the Internet, or over corporate extranets, risks impersonation and tampering. *thawte* Code Signing Certificates protect against these hazards.

The *thawte* Code Signing Certificate provides greater assurance about the identity of a publishing organization. It is designed to represent the high level of assurance provided by today's retail channels for software.

thawte Developer Certificates are used to sign Java applets for the Java 2 plugin, Navigator/JVM 1.1.x and Microsoft Authenticode. They can also be used for signing .cab, .exe, and .dll files, and for signing Office 2000 Macro and Internet Explorer Object files.

thawte offers a number of different types of code signing certificates, as well as one that can be used across the board. It is possible to buy one Code Signing Certificate from *thawte* and to use it for Microsoft AuthentiCode, Microsoft Office 2000/VBA Macro Signing, Netscape Object Signing, and Marimba Channel Signing, and with some tweaking it can be used to sign Java 2 applets created with particular versions of the JDK.

4. Does thawte certify your code?

No. *thawte* issues you as the developer with a certificate once we have verified your particulars. We certify your identity, not the quality or intent of your code. However, if there is any indication that a developer abuses code signing infrastructure his/her certificate(s) will be revoked, and never issued again.

5. How can customers identify your digital signature?

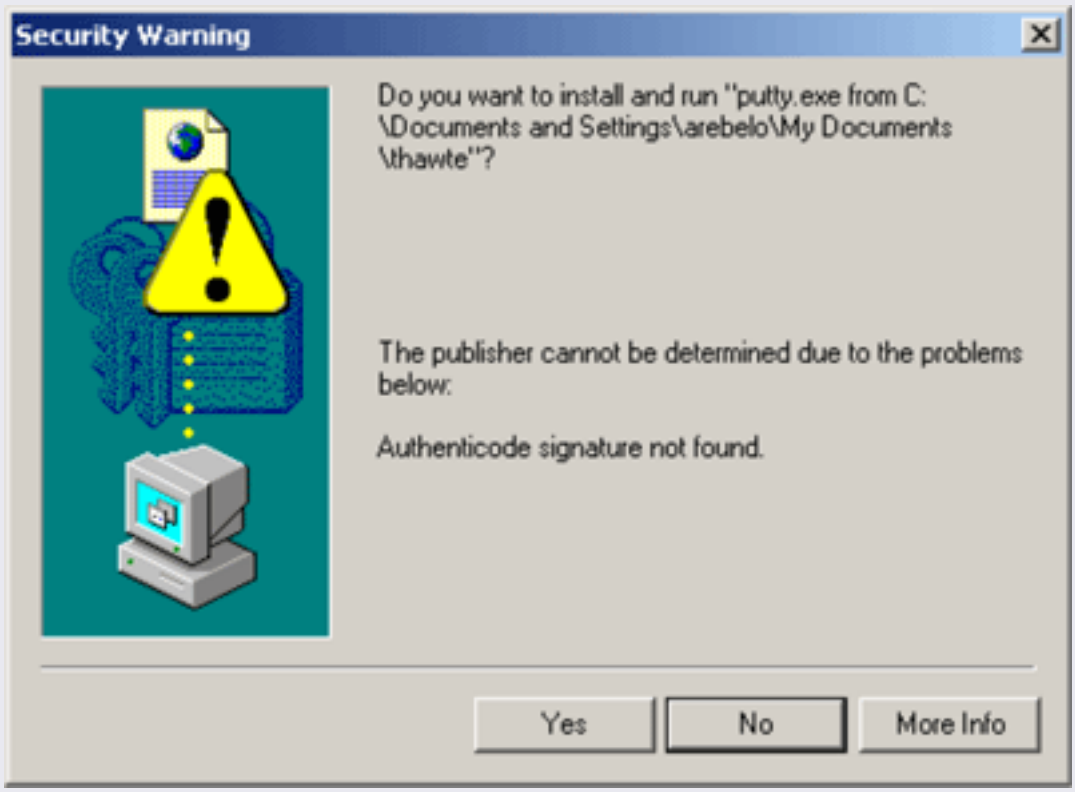
5.1 Microsoft Authenticode

Microsoft client applications such as Internet Explorer, Exchange, Outlook and Outlook Express have security features that incorporate Authenticode. These applications are often used to obtain other pieces of software. In a component model such as ActiveX or Java this happens frequently, often without the end user being aware of it. For example, when a user visits a web page that uses executable files to provide animation or sound, code is often downloaded to the end user's machine to achieve the effects. While this may provide substantial value, users risk downloading viruses or code from a disreputable publisher.

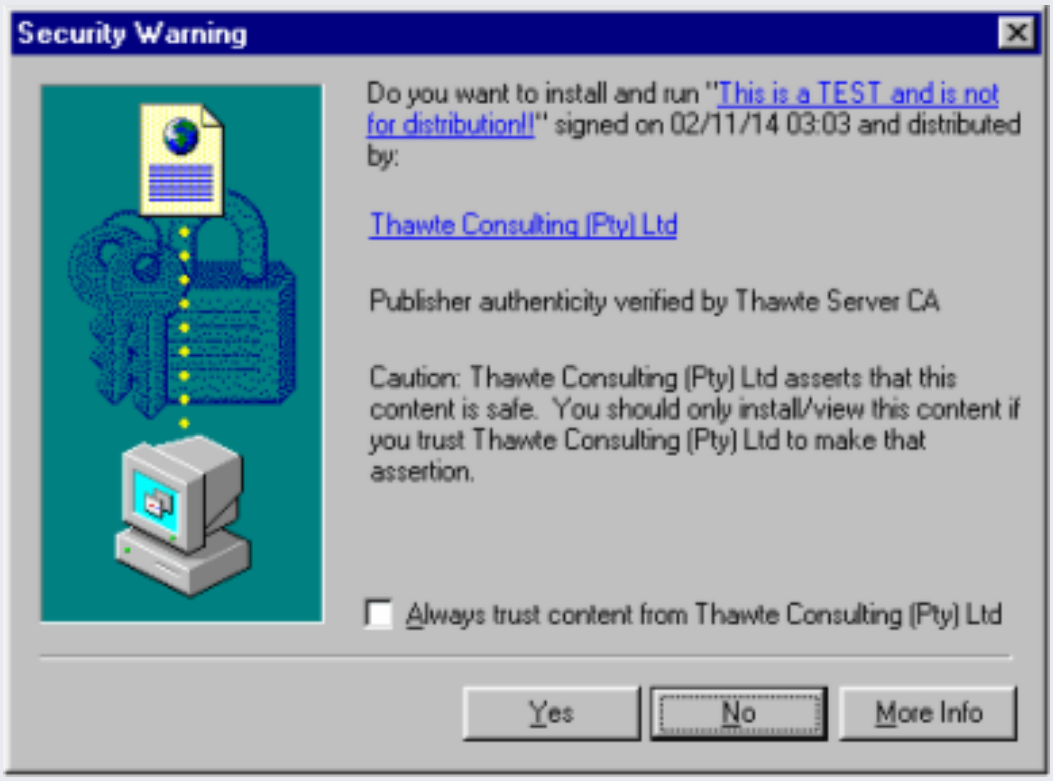
If an end user of one of these applications encounters an unsigned component distributed via the Internet, the following will occur:

If the application's security settings are set on "**High**," the client application will not permit the unsigned code to load.

If the application's security settings are set on "**Medium**," the client application will display a warning like this screen.



On the other hand, if a user encounters a signed applet or other code, the client application will display a screen similar to this one:



Through Authenticode, the user is informed:

- of the true identity of the publisher (in this case thawte Consulting (Pty) Ltd);
- that the authenticity of the above information is provided by thawte Server CA (thawte Consulting).

The user can choose to trust all subsequent downloads of software from the same publisher. The user can also choose to trust all software published by commercial publishers that have been certified by *thawte*.

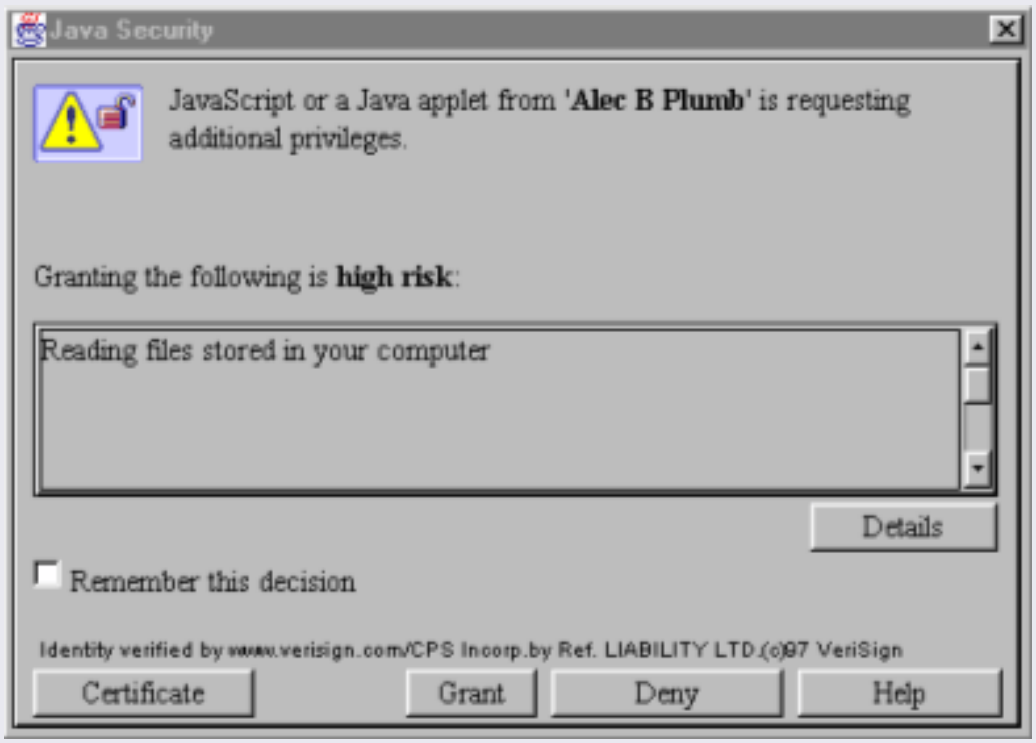
Simply by clicking the "**More Info**" button, the user can inspect the certificate and verify its validity.

5.2 Netscape Object Signing

Netscape Communicator and other popular client applications come with security features that recognize Object Signing. These applications are often used to obtain other pieces of software from networks, sometimes without the end user requesting it.

When Communicator encounters a software component that is trying to gain access to the user's machine, it automatically checks to see if there is a recognized digital signature with that software.

If the code is signed with a Netscape Object Signing Certificate, the following dialog box will appear:

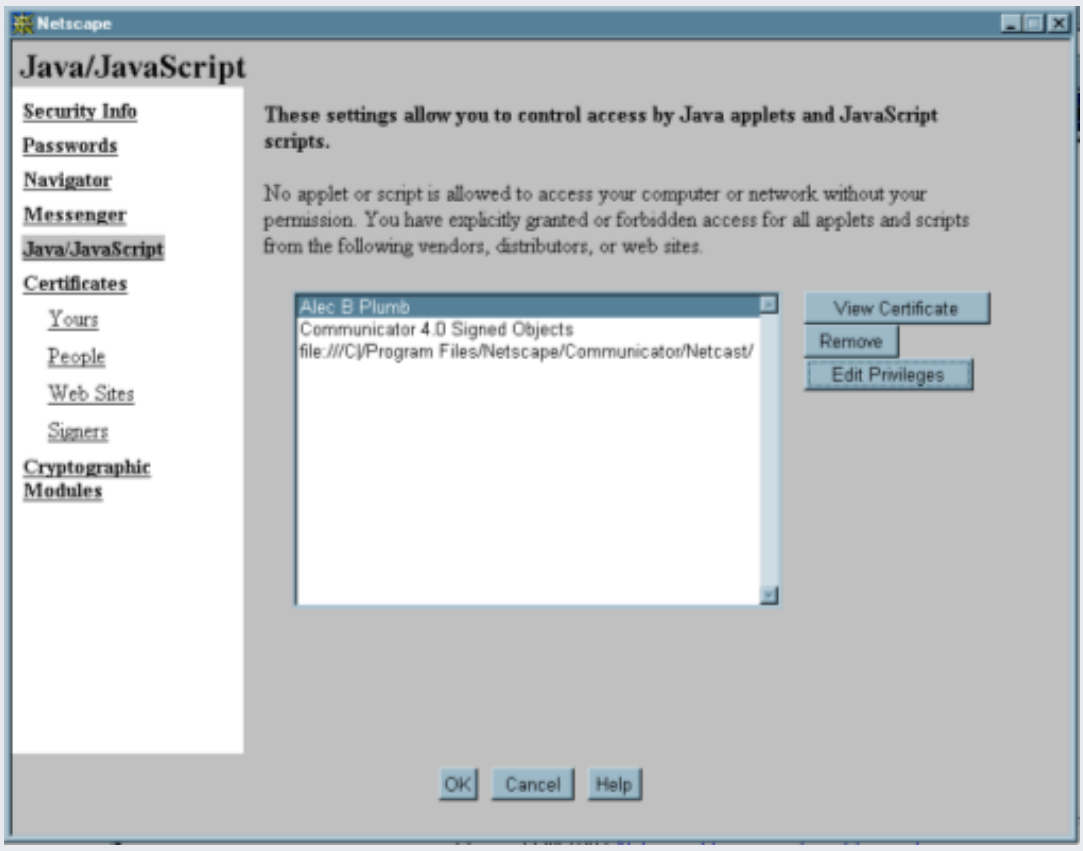


Through Object Signing, the user is informed:

- of the true identity of the publisher;
- the type of access requested by the software; and
- that the authenticity of the above information is provided, in this case, by VeriSign.

The end user can choose to grant or deny the requested privileges, or to view the certificate used to sign the code. Communicator provides an estimated level of risk (high, medium or low) associated with the privileges requested, and the user can learn more about this risk by clicking “Details”.

By selecting “Remember this decision,” the user saves the digital signature of that software publisher so that Communicator will recognize it in future. When the end user’s Netscape browser encounters a signed applet or other code with a recognized signature, the browser automatically allows the code to run, remembering the privileges it has previously been granted, without interrupting the user. The user can at any time add, delete or edit the privileges he/she wants to grant to publishers. By clicking the security icon in the main Communicator toolbar, the user displays the following screen:



5.3 Microsoft Office and VBA

Microsoft Word, Excel, PowerPoint and Outlook 2000 applications support signing and verifying digital signatures on VBA code. Other third party applications with VBA 7.0 may also support digital signatures in VBA code. For more information regarding your application’s support and usage of code signing certificates contact your software vendor. If an end user of one of these applications encounters an unsigned VBA macro, the following will occur:

- If the application's security settings are set on "High," the client application will not permit the unsigned code to run.
- If the application's security settings are set on "Medium," the client application will display a warning asking the user whether (s)he wants to enable or disable this unsigned code.

By contrast, if a user encounters signed VBA code in a file, the user is informed:

- of the true identity of the publisher (in this case Microsoft Corporation); and
- that there is no problem with the certificate (the absence of additional warnings).

The user is also able to view the certificate and can choose to trust all subsequent VBA code from the same publisher source.

6. Time Stamping

Because key pairs are based on mathematical relationships, which can theoretically be cracked with a great deal of time and effort, it is a well-established security principle that digital certificates should expire. A digital certificate is valid for a year. However, your code might be in use for many years.

Time stamping your code will alert a user that the code was signed while your certificate was still valid. When you sign your code, it should be possible to have that signature time stamped by an independent party. While thawte does not run a time stamping server, you can use VeriSign time stamping server by adding:

"http://timestamp.verisign.com/scripts/timstamp.dll"

to the signcode command line. *thawte* appreciates this cooperation with VeriSign.

Notes:

Netscape implements time stamping by default, but the time stamp is not verified, so you need to re-sign code that resides on the Netscape platform.

Sun's JDK does not currently support time stamping.

7. How to use the Multiple Code Signing Certificate

You can take advantage of the interoperability of *thawte* Code Signing Certificates.

This is extremely useful should you wish to use the same certificate to sign code for multiple browsers/file types. To do this, you have to follow a particular progression from one application to another as follows:

A. Request a Microsoft Authenticode Certificate or

- Fill in the location on your hard drive where you would like to store the private key
- If the field is left blank it will be stored in the registry and cannot be imported to .pvk and .spc files (certain signing applications only look for keys in that format.)
- Save .pvk file to your hard drive for use as a multi-purpose certificate

B. Move the certificate and private key to the registry with PVKIMPRT.exe

- The private key can only be imported into the registry with a Microsoft utility called pvkimprt.
- For more information on the usage and download instructions for this tool go to "http://www.office.microsoft.com/downloads/2000/pvkimprt.aspx".
- Moving the certificate and private key to the registry allows you to sign Office 2000 and VBA Macros.
- pvkimprt.exe download: The file that you'll download from Microsoft is a elfextracting archive which, when executed without any options, will install the real 'pvkimprt.exe' into a directory on your path.
- pvkimprt.exe usage: The order in which you list the files is important. First the SPC file and then the PVK file.

C. Export the certificate and key to a p12

- In Internet Explorer click on “View > Internet Options > Contents > Certificates”.
- Export the certificate to a .pfx (PKCS#12) file.
- During the process, please indicate in the checkbox that you would like to export the private key as well.
- For a detailed view of this procedure take a look at: http://www.thawte.com/support/code/tech.html

D. Import into Netscape

- In Netscape Navigator, click on the Security button or go to your security
- Click on: “Certificates > Yours > Import”.
- Follow the instructions to add the PKCS#12 file to your Netscape KeyStore.
- A side effect of importing an MSIE .p12 file is that the "friendly name" that appears in the Netscape cert list, and with which you reference the certificate, is definitely not friendly.
- For detailed instructions, please consult: http://www.thawte.com/support/code/index.html

8. Useful URLs

For more detail on thawte's Code Signing Certificates, please visit:

http://www.thawte.com/codesign/index.html

Common problems experienced with Code Signing Certificates are dealt with in our FAQs:

http://www.thawte.com/support/code/index.html

Buy Code Signing Certificates:

http://www.thawte.com/buy/

9. What Role Does thawte Play?

thawte Technologies is a Certification Authority (CA) which issues Digital Certificates to organizations and individuals worldwide. thawte verifies that the company ordering the certificate is a registered organization and that the person in the company who ordered the certificate is authorized to do so.

thawte also checks that the company in question owns the relevant domain. *thawte* digital certificates interoperate smoothly with Apache and the latest software from Microsoft and Netscape, so you can rest assured that you purchase of a *thawte* Digital Certificate will give your customers confidence in your system and integrity – they will feel secure about transacting online.

10. The Value of Authentication

Information is a critical asset to your business. To ensure the integrity and safety of your information, it is important to identify with whom you are dealing, and the data you are receiving is trustworthy. Authentication can help establish trust between parties involved in all types of transactions by addressing a unique set of security issues including:

Spoofing:

The low cost of website design and the ease with which existing pages can be copied makes it all too easy to create illegitimate websites that appear to be published by established organizations. In fact, con artists have illegally obtained credit card numbers by setting up professional looking storefronts that mimic legitimate businesses.

Unauthorized Action:

A competitor or disgruntled customer can alter your website so that it malfunctions or refuses to service potential clients.

Unauthorized Disclosure:

When transaction information is transmitted “in the clear”, hackers can intercept the transmissions to obtain sensitive information from your customers.

Data Alteration:

The content of a transaction can be intercepted and altered en route, either maliciously or accidentally. User names, credit card numbers and currency amounts sent “in the clear” are all vulnerable to alteration.

11. Contact *thawte*

Should you have any further questions regarding the content of this guide or *thawte* products and services, please contact a Sales Advisor:

E-Mail: sales@thawte.com
Telephone: +27 21 937 8902
Fax: +27 21 937 8967