Securing Your Software

for Web Distribution

A Step-by-Step Guide to Digitally Signing Your Software Using PackageForTheWeb and InstallFromTheWeb with VeriSign Digital IDs.

1. Introduction

The rapid and continuing growth of electronic software distribution and commerce shows no sign of slowing down. Clearly the potential for distributing software via the Internet is enormous. Convenience is the primary advantage to conducting business via the Internet -- customers can download and install products quickly and reliably without even leaving their desks. Plus, the costs of conventional distribution are eliminated, as are time-consuming interactions with publishers and distributors.

CEO of IBM, Lou Gerstner said he thinks the market for Internet commerce will hit $200 billion a year by the end of the century. Gerstner, a keynote speaker at the CeBIT information technology fair in Germany, said: "I believe that's a conservative forecast."

"By the year 2002, electronic commerce between businesses in the United States alone will exceed $300 billion." - President Clinton.

However, customers are concerned about the authenticity or legitimacy of the products they obtain from the Internet. In a conventional retail setting, customers can tell who published the software, and see whether the package has been tampered with. Internet distribution seems to lack the physical reassurance of sealed software packages. The Internet also lacks the subtle familiarity provided by a retail setting, shelf space, and packaging. Without reliable information about the person or organization responsible for producing the software, customers are wary of making purchase decisions.

To alleviate these issues, InstallShield's **InstallFromTheWeb**™ and **PackageForTheWeb**® now feature VeriSign security and authentication capabilities. These market leading Internet distribution products allow software developers to digitally sign their code using **VeriSign Digital IDs** and Microsoft Authenticode™ technology. For software developers distributing via the Web, signing code is the electronic equivalent to shrink-wrapping software boxes. Online customers are assured of the identity of the software publisher, and provided with the ultimate confidence that no alterations have been made to the software since the time of publication.

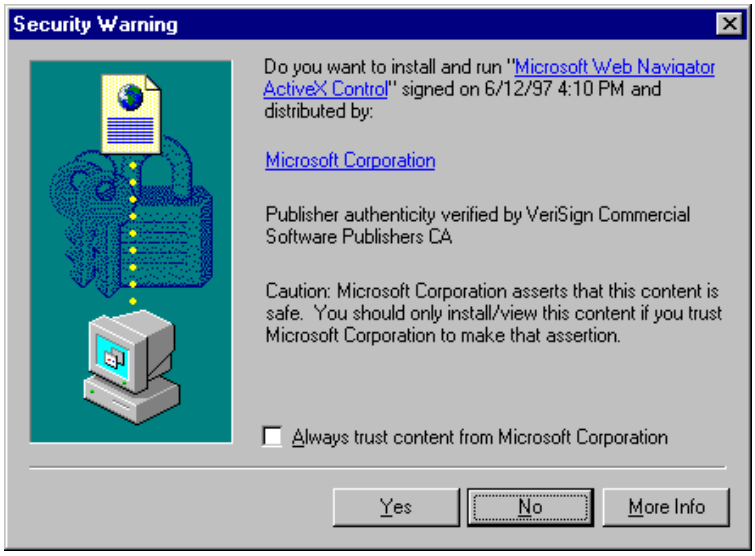
2. What Is Microsoft Authenticode?

Authenticode is a proven technology distributed by Microsoft, allowing software publishers to attach a digital signature to their software products. This digital signature, created using a Developer ID from VeriSign, allows the publisher to verify his or her identity to on-line clients.

When customers download software that is signed using Microsoft Authenticode with a VeriSign Software Developer ID, they are assured that the software they are buying comes from the individual or company whose signature appears on it, and has not been altered since the time it was signed. When code is downloaded, before installation on a user's system, a dialog box appears that assures the user of the authenticity of the code he or she is about to install.

Users benefit from this software accountability because they are assured of the identity of the software publisher, and that the product they are buying hasn't been tampered with. In case the software performs unexpectedly, users know which publisher to contact for further information.

Software developers and Webmasters benefit from Authenticode because it puts trust in their name and makes their products virtually impossible to falsify. By signing code, developers build a trusted relationship with users, who are more likely to download signed software from that publisher or Web site with confidence. With Microsoft Authenticode, developers who have a Software Developer ID can create exciting Web pages using signed ActiveX® controls, signed Java™ applets, or other signed executables. Users can make educated decisions about what software to download with the assurance of knowing who published the software and that it hasn't been tampered with.



3. What Is a Digital ID?

A Digital ID, also known as a digital certificate, is a form of electronic credential for the Internet. Similar to a driver's license, employee ID card, or business license, a Digital ID is issued by a trusted third party to verify the identity of the ID holder. The third party that issues certificates is known as a Certification Authority (CA).

Digital ID technology is based on the theory of public key cryptography. In public key cryptography systems, every entity has two complementary keys -- a public key and private key -- that function only when they are held together. Public keys are widely distributed to users, while private keys are kept safe and only used by their owners. Anything encrypted with the public key can only be decrypted with the private key. The public key can only successfully decrypt anything that was encrypted by the corresponding private key. For more information on public keys and private keys, please visit:

http://www.verisign.com/developers/authenticodefaq.html

The purpose of a Digital ID is to reliably link a public key with its owner. When a CA such as VeriSign issues Digital IDs, it verifies that the owner is not claiming a false identity. Just as when a government issues you a passport it is officially attesting the fact that you are who you say you are, when a CA issues you a digital certificate, it is putting its name behind the statement that you are the rightful owner of your public key.

A Digital ID is valid only for the period of time specified by VeriSign. The ID contains information about its activation and expiration dates. VeriSign also has the right to revoke (cancel) any certificate it has issued and maintains a list of revoked certificates. VeriSign publishes a list of all revoked certificates, called a Certificate Revocation List (CRL), so that anyone can further confirm the validity of any Digital ID.

Certification Authorities

Certification Authorities, such as VeriSign, are organizations that issue digital certificates to applicants whose identity they are willing to vouch for. Each certificate is linked to the certificate of the CA that signed it.

As the Internet's leading Certification Authority, VeriSign is responsible for the following:

- Publishing the criteria for granting, revoking, and managing certificates.
- Granting certificates to applicants who meet the published criteria.
- Managing certificates (for example, enrolling, renewing, and revoking them).
- Storing VeriSign's root keys in an exceptionally secure manner.
- Verifying evidence submitted by applicants.
- Providing tools for enrollment.
- Timestamping digital signatures.
- Accepting the liability associated with these responsibilities.

Authenticode and VeriSign Digital IDs

Authenticode uses digital signature technology to assure users of the origin and integrity of software. In digital signatures, the private key generates the signature, which is validated by its corresponding public key. To sign documents, the signing tool creates a message digest, which is a one-way hash of the document.

The process is outlined below:

1. The publisher obtains a Software Publisher Digital ID from VeriSign.
2. The publisher creates software.
3. Using InstallFromTheWeb or PackageForTheWeb, the publisher adds the Digital ID to the software during the Web-enablement process.
4. The publisher distributes software over network.
5. End user's browser encounters the package.
6. End user's browser examines the publisher's Digital ID. Using the VeriSign Public Key, the end user verifies the authenticity of the ID.
7. Using the public key contained within the publisher's ID, the end user's browser decrypts the hash.
8. End user's browser runs the code through the same hashing algorithm as the publisher, creating a new hash.
9. End user's browser compares the two hashes. If they are identical, the end user has assurance that the publisher signed the code, and that the code hasn't been altered since it was signed. If they are not identical, the user is warned that the code may have been tampered with.

The entire process is seamless and transparent to end users. Only a message that the content was signed by its publisher and verified by VeriSign is displayed.

Timestamping

Key pairs are based on mathematical relationships which can theoretically be "cracked" with a great deal of time and effort. Therefore it is a well-established security principle that digital certificates should carry an expiration date.

For this reason, your VeriSign Digital ID will expire one year after it is issued. However, most software is intended to have a lifetime of longer than one year. To avoid the need for publishers to re-sign software every time their certificate expires, VeriSign provides a timestamping service for Authenticode users. When you sign code, a hash of your code will be securely sent to VeriSign to be timestamped. As a result, when your code is downloaded, clients will be able to

distinguish between code signed with an expired certificate and code signed with a certificate which was valid at the time the code was signed, but which has subsequently expired.

This means that you will not need to worry about re-signing code when your Digital ID expires.

4. Who needs a Software Publisher ID?

Any publisher who plans to distribute code or content via the Internet or corporate Extranets risks impersonation and having his or her code tampered with. VeriSign Software Publisher IDs for Microsoft Authenticode protect against these hazards.

A **Commercial Software Publisher Digital ID** is designed for *Commercial Software Publishers*. Commercial Software Publishers are companies and other organizations that publish software. This class of Digital IDs provides greater assurance regarding an organization's identity and legitimacy, much like a business license.

When you are ready to acquire your Digital ID for use with InstallShield's products, please visit http://www.verisign.com/installshield.

5. How do I Sign my software products?

The following instructions provide an overview of obtaining and using Microsoft Authenticode and a Software Publisher's ID from VeriSign:

Step 1: Obtain PackageForTheWeb or InstallFromTheWeb

Both PackageForTheWeb and InstallFromTheWeb are available directly from InstallShield Software Corporation and software tools resellers and distributors worldwide. PackageForTheWeb is also included with the InstallShield Professional.

Email:	Sales@installshield.com
Sales:	1.847.240.9111
Toll-Free:	1.800.374.4353
WWW:	http://www.installshield.com/isorder

You should be running Internet Explorer version 4.0 or later in order to use the latest release of Authenticode.

Step 2: Apply for an Authenticode Software Publisher's ID from VeriSign.

Go to **http://digitalid.verisign.com/developer/ms_pick.htm** to begin enrollment for a Software Publisher's Digital ID.

When applying for a Software Publisher's ID, your browser will generate a private key. You should store this private key (*.pvk) on a floppy disk that is stored in a safe deposit box or other secure location. Please make a back-up copy of this private key, as you will need this key to sign code. This key is never sent to VeriSign, so if you lose this private key, you will be unable to sign code. If this key is lost or stolen, please contact VeriSign immediately.

Step 3: Pick Up Your Digital ID

Once you have completed the application process, VeriSign takes exhaustive measures to verify your identity. For commercial publishers, VeriSign performs a rigorous background check, so it will take approximately 3-5 business days to verify your information and issue your Digital ID.

Once verification is complete, VeriSign will email you a PIN (Personal Identification Number). Follow the instructions in this e-mail to pick up your Digital ID. Save your Digital ID as a file (e.g. MyCredentials.spc).

You must use the same machine to apply for and retrieve your Digital ID. You can then use the private key and Digital ID to sign files on a different machine.

Step 4: Sign Your Files

You can now sign your .exe, or .cab, .ocx, or .dll file. To sign you will use either **InstallFromTheWeb** or **PackageForTheWeb**. You will also need your Digital ID file (*.spc) and the diskette containing your private key (*.pvk).

Step 5: Test Your Signature

To check your signature before distributing your file launch your installation. If your signing process was successful, a dialog box will be displayed:

This dialog contains the name of the code, the date and time at which the code was signed, by whom it was signed and authentication of the publisher. When Internet Explorer downloads this file from a Web site, it will display the same certificate to the user. If the file is tampered with in any way after it has been signed, the user will be notified and given the option of refusing installation.

6. InstallShield Electronic Software Distribution Products

As the world's leading developer of distribution and deployment software, InstallShield Software Corporation features two products that enable you to easily build your online business. InstallFromTheWeb and PackageForTheWeb allow you to distribute your applications to your the end users over the Internet. Furthermore, both InstallFromTheWeb and PackageForTheWeb allow developers to attach digital signatures to their software.

InstallFromTheWeb

InstallFromTheWeb makes obtaining software from the Internet friendlier for developers, Webmasters and end users. When you Web-enable your installations with InstallFromTheWeb, your end users can experience a seamless and trouble-free software download and installation process directly from your Web site. A single click of the install button on your Web site launches your software installation automatically.

InstallFromTheWeb offers great benefits such as these:

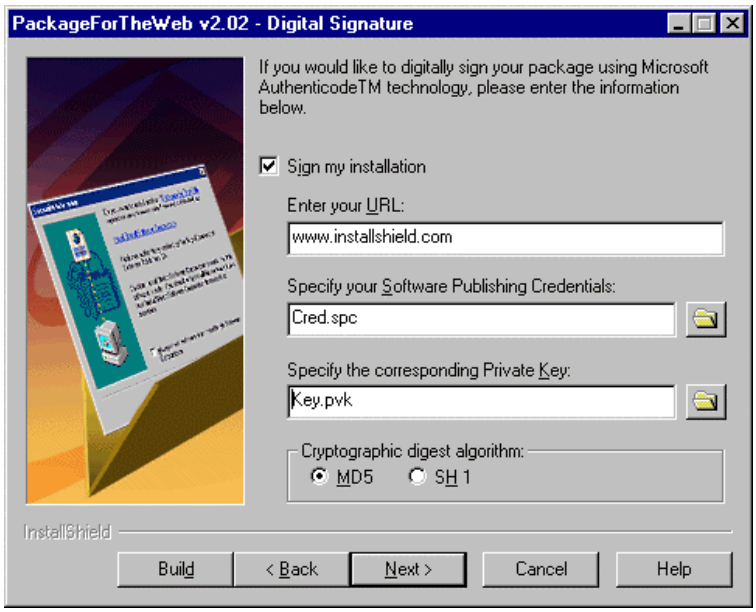
- **Error Recovery** - When the user loses his connection with an InstallFromTheWeb installation, he does not have to start the download over. Upon retrying installation, InstallFromTheWeb will download only the files that haven't already been installed.

- **Selective Component Download** - End users have the option to download and install only the components they want, rather than the entire application.

- **Dynamic Reconnect** - If a connection to a remote site breaks during download, InstallFromTheWeb’s dynamic reconnect can instantly and silently jump to another available mirror site to obtain the files, so the download continues smoothly for the end user.

PackageForTheWeb

PackageForTheWeb provides developers with a single easy solution for packaging files, applications, and ActiveX controls for Internet distribution. A simple Wizard-driven interface will allow you to quickly create and digitally sign a 32-bit self-extracting Executable or Cabinet file.



Signing your Code

If you choose to digitally sign your distribution, you are presented with the Digital panel. Here you enter information provided for you by a Certificate and select an algorithm to encrypt information about the package's content and software credential information.

The algorithm that you choose creates a unique digest of your package and authentication information which is then signed with the private keyyou provide. PackageForTheWeb or InstallFromTheWeb uses Microsoft Authenticode Technologyto append this signature to your package.

If you digitally sign your software, end users are presented with a digital certificate when your cabinet is downloaded to their system.

To digitally sign a package, perform the following steps:

Step 1:Enter Product Name

Make sure that you have entered a product name in the Product Information panel as PackageForTheWeb or InstallFromTheWeb uses this information to digitally sign your installation.

Step 2: Enter your URL

Enter a fully qualified URL, for example, http://www.mydomain.com. This URL is used in your digital certificate to link to a location you

would like end users to visit in order to learn more about your product, organization, or company.

If you would like to digitally sign your distribution, you must complete the Enter Your URL field. If this field is left blank, you will receive the following error in the Build Window:

You can use the Browse folder button to navigate to the location of the .spc file provided by a Certificate Authority or enter the path to the file. \

Step 3: Declare the location of your Private Key

You may use the Browse folder button to navigate to the location of the .pvk file provided by a Certificate Authority or enter the path to the file.

Step 4: Select a Cryptographic Digest Algorithm

A cryptographic digest algorithm is used to encrypt information gathered about your PackageForTheWeb or InstallFromTheWeb project entered in the Digital Signature panel before digitally signing the package with your private key. Choose between MD5 and SH1 digest algorithms.

End users need Internet Explorer 3.0, 3.01, 3.02 and the Authenticode 2.0 security update or Internet Explorer 4.0 in order to view your digital certificate via the Web. Please visit www.microsoft.com/security for information on the latest security update. On this site you may determine if you have the Authenticode update installed (if you are using Internet Explorer) and obtain tools to make sure that your end users have the update installed.

When you digitally sign a package, signcode.exe included in PackageForTheWeb or InstallFromTheWeb opens an Internet connection and references a .dll on VeriSign's Web site to timestamp the signature. Therefore, it is necessary that you have Internet access if you are going to digitally sign a package.