VeriSign®

WHITE PAPER

How to Digitally Sign Downloadable Code for Secure Content Transfer

VeriSign®

WHITE PAPER

CONTENTS

How to Digitally Sign Downloadable Code for Secure Content Transfer

+ What Is Code Signing?

Code Signing, sometimes called Object Signing, is a technology that has the ultimate objective of helping developers to sell more software online. Code Signing helps by making customers just as confident about installing and using software purchased via the Internet as they are with software purchased in person. When people buy software in a store, the safety of installing and using that software is obvious. They can observe who published the software, and they can see whether the package has been opened. These factors enable them to make decisions about which software to purchase and how much to trust that software.

Contrast this to a customer downloading software from the Internet where they do not have the same confidence-building experience. Perhaps they even receive a message warning them about the dangers of using the software, which diminishes their confidence even more. The Internet lacks the tangible information provided by packaging, shelf space, shrink wrap, and the like. Without an assurance of the software's integrity or its publishing credentials, customers have difficulty deciding how much to trust it. They can be justifiably concerned that it might be from a source other than that stated or might have been tampered with, and may therefore have viruses or other unwanted code. Reluctant to proceed with their downloads, people may well go to a retail outlet instead—or simply not purchase the software at all. This represents a loss of business for the Internet retailer and an inconvenience or worse for the customer, who might not even be able to find it on store shelves.

VeriSign offers a solution to these issues with a solution that will digitally "shrink-wrap" the software with a digital signature. The digital signature verifies the authenticity of the publisher and the integrity of the product.

Digital signatures can be created with a VeriSign® Code Signing Digital Certificate and a platform signing utility. VeriSign provides digital certificates for the following:

+ Microsoft® Authenticode, Office and VBA,
+ Sun® Java, and
+ Netscape® Object Signing

When customers download software signed with a VeriSign Code Signing Digital 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

Users benefit from this software accountability because they know with certainty who published the software and that the code has not been tampered with. In the extreme case that software performs unacceptable or malicious activity on their computers, users can also pursue recourse against the publisher. This accountability and potential recourse serve as a strong deterrent to the distribution of harmful code.

Developers and Web masters benefit from using VeriSign Code Signing Digital Certificates because they are thereby engendering trust in their names and making their products harder to falsify. By signing code, developers build a trusted relationship with users, who then learn they can confidently download signed software from that publisher or Web site at any time.

+ Who Needs Code Signing Digital Certificates?

Any software publisher who distributes code or content over the Internet or through an extranet risks impersonation and tampering with consequent loss of business and reputation. VeriSign Code Signing Digital Certificates protect against these hazards.

VeriSign Code Signing Digital Certificates have a Class 3 assurance level to meet the needs of commercial software developers. This class of digital certificates provides assurance of an organization's identity and legitimacy, much like a business license, and is designed to represent the level of assurance provided today by retail channels for software.

+ What Does Code Signing Look Like to End Users?

End user platforms come with security features that recognize Code Signing. Some applications may attempt to obtain other pieces of software from networks, sometimes without the user requesting them. For example, when users visit a Web page that uses executable files to provide animation or sound, their browsers download code to their machines to achieve the desired effects. Knowing that this could result in viruses or other unwanted code, users need reassurance that the software will be safe before granting permission to perform the download.

When software is being downloaded to the user's machine, the security features automatically check to see if there is a recognized digital signature from a VeriSign Code Signing Digital Certificate (or other recognized source). If the platform sees such a digital signature, it provides this information to users in the form of a dialog box that (a) indicates the software has not been modified, (b) identifies the publisher, and (c) affirms that VeriSign attests to the authenticity of the publisher. The dialog box also states other information that varies somewhat from platform to platform as described below. Users can then opt to proceed with the download with confidence or gain additional assurance by viewing the VeriSign Code Signing Digital Certificate.

+ What Are the Differences Between Platforms?

The following three vendors' platforms differ slightly in implementation as described below.

Microsoft® Authenticode and Microsoft® Office/Visual Basic for Applications (VBA)
Microsoft client applications such as Internet Explorer, Exchange, PowerPoint, and Outlook come with security features that incorporate Authenticode for processing digital signatures. If Authenticode encounters a signed component, the user is informed about the safety of the code and the authenticity of the supplier as described above. If however, Authenticode encounters an unsigned VBA macro or any unsigned component distributed by 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 run.
- If the application's security settings are set on "Medium," the client application will display a warning, which asks whether the user wants to install and run this unsigned code or not.

Users can choose to trust all subsequent downloads of software from the same publisher. They can also choose to trust all software published by commercial publishers that sign their code with VeriSign Code Signing Digital Certificates.

Netscape® Object Signing

Netscape Communicator and other popular client applications come with security features that recognize Object Signing. When Communicator encounters a signed component attempting to gain access, it not only presents a dialog box as described above but goes one step further in helping the end user choose whether to grant or deny the requested privileges by estimating a level of risk (i.e., high, medium, or low) associated with these privileges. The user can learn more about this risk by clicking "Details."

By selecting "Remember this decision," the user saves the digital signature of the software publisher so that Communicator will recognize it in the future. When the end-user's Netscape browser encounters a signed applet or other code with a recognized signature, the browser automatically allows that code per the privileges it has previously been granted, without interrupting the user. Users can add, delete, or edit the privileges they want to grant to publishers at any time.

Sun® Java

Applications that run Java applets and applications running on the Java Runtime Environment (JRE) come with security features that recognize Code Signing.

As with Netscape, the Sun Java platform's dialog boxes provide the user with an estimated level of the risk (high, medium, or low) associated with the requested privileges and a means for viewing the details included in the software developer's certificate.

+ Conclusion

With VeriSign Code Signing Digital Certificates, developers can create Web pages using signed Java applets, plug-ins, or other executables, and users can make educated decisions about which software they want to download.

VeriSign and its partners Microsoft, Netscape, and Sun Microsystems are committed to making the Internet a secure and viable platform for online commerce and the distribution of content. With Code Signing and VeriSign Code Signing Digital Certificates, an application is as safe and trustworthy to customers as it would be if the author had it shrink-wrapped and sold on a store shelf. As a result, developers benefit by building trust with their customers which can lead to increased sales over their online channel. As the practice of signing a company's software product with VeriSign Code Signing Digital Certificates becomes more and more commonplace, customers will increasingly look for this level of reassurance before performing downloads. This may results in an adverse impact on sales for vendors who fail to use them and a heightened value for those who do.

For more information, visit www.verisign.com or call 1-866-893-6565 or 1-650-426-5112, option 3.

+ About VeriSign

VeriSign is the trusted provider of Internet infrastructure services for the digital world. Billions of times each day, companies and consumers rely on our Internet infrastructure to communicate and conduct commerce with confidence.

Visit us at www.VeriSign.com for more information.

00025986 4-29-2008