



CHANNEL PARTNER PROGRAM

# HOW TO DIGITALLY SIGN DOWNLOADABLE CODE FOR SECURE TRANSFER



PARTNER PROGRAM



PARTNER PROGRAM

CHANNEL PARTNER  
PROGRAM

## CONTENTS

- 1 WHAT IS CODE SIGNING AND WHY IS IT IMPORTANT?
- 2 WHO NEEDS CODE SIGNING CERTIFICATES?
- 2 WHAT DOES CODE SIGNING LOOK LIKE TO END USERS?
- 2 WHAT ARE THE DIFFERENCES BETWEEN PLATFORMS?
- 3 CONCLUSION
- 4 ABOUT VERISIGN





PARTNER PROGRAM



CHANNEL PARTNER PROGRAM

## HOW TO DIGITALLY SIGN DOWNLOADABLE CODE FOR SECURE TRANSFER

### WHAT IS CODE SIGNING AND WHY IS IT IMPORTANT?

Code Signing, sometimes called Object Signing, is a technology that has the ultimate objective of helping developers to distribute 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 customers 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 publisher's 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 contain viruses or other forms of malware. 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.

To increase software downloads, preserve their business reputation, and build a trusted relationship with customers, software publishers must protect their products from those who would alter it with malicious intent. These publishers must show users that they have implemented strong

protective measures. To maximize software adoption and online sales, they also need to allow their applications to run without requiring that users alter their security settings while avoiding security warning messages about unknown sources that scare away customers.

VeriSign offers a solution to these challenges 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 Certificate and a platform signing utility. VeriSign provides digital certificates for the following:

- Microsoft® Authenticode®, Office and VBA,
- Sun™ Java™, and
- Adobe® AIR™

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

- Content Source—The publisher identified in the code signing certificate is a valid company.
- Content Integrity—The software has not been altered or corrupted since it was signed.

---

### AT A GLANCE

- Create end user confidence and protects your brand
  - Eliminate disruptive security alerts and reduce support inquiries
  - Increase adoption of downloadable software
  - Lower total cost of certificate ownership
  - Support more platforms than any other signing solution
- 





## PARTNER PROGRAM



## CHANNEL PARTNER PROGRAM

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 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.

VeriSign's root certificates come pre-installed on most end users' Windows and Mac OS computers and are trusted by these operating systems. VeriSign supports more platforms than any other signing solution with a timestamp option, which enables users to verify that a code signing certificate was indeed valid at the time of initial signature. In removing the need to constantly renew the certificate, time-stamping significantly reduces a developer's administrative time and effort and thus decreases a certificate's total cost of ownership.

### WHO NEEDS CODE SIGNING CERTIFICATES?

Any software publisher that 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 Certificates protect against these hazards. VeriSign Code Signing 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 employs 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 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) may affirm 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 Certificate.

### WHAT ARE THE DIFFERENCES BETWEEN PLATFORMS?

The 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.





## PARTNER PROGRAM



## CHANNEL PARTNER PROGRAM

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 Certificates.

### Sun™ Java™

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

When JRE 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."

### Adobe® AIR™

Adobe requires that all Adobe AIR-based applications be digitally signed.

When a user attempts to install an AIR application that has been signed by a certificate from a known certificate authority, an Adobe AIR installation dialog box will appear, informing the user of the true identity of the publisher and extent of the application's system access.

If a user attempts to install an AIR application that has been signed by a certificate from an unknown authority, or a self-signed certificate, the dialog box informs users that the publisher identity is unknown. It asks users to confirm that they wish to proceed, reminding them of the security risks associated with doing so.

## CONCLUSION

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

VeriSign and its partners Microsoft, Sun Microsystems, and Adobe 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 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 Certificates becomes more and more commonplace, customers will increasingly look for this level of reassurance before performing downloads. This may result in an adverse impact on sales for vendors who fail to use them and a heightened value for those who do.

## 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](http://www.Verisign.com) for more information.





PARTNER PROGRAM

CHANNEL PARTNER PROGRAM

**VERISIGN, INC.**

USA Headquarters  
487 East Middlefield Road  
Mountain View, CA 94043 USA

P 650-961-7500  
F 650-961-7300

European Headquarters  
8, Chemin de Blandonnet  
Vernier-geneva CH-1214  
Switzerland

P + 41-22-545-0200  
F + 41-22-545-0300

VeriSign, Inc. and its Partners are each independent contractors, and nothing herein contained shall be construed to imply the existence of a partnership or joint venture between them, nor to make either one an agent of the other. The use of the term "Partner" is not intended in any way to constitute any type of legal partnership whatsoever between VeriSign, Inc. and Partner. The relationship between VeriSign, Inc. and Partner is that of independent contractor only, and is NOT employer-employee, partner, principal-agent or joint venture. VeriSign does not make any representations or endorsement of any of the products or services listed here which are provided by non-VeriSign sources. That information was provided by the named source, and VeriSign has made no effort to independently verify the products or services. Users of this information are responsible for checking with the non-VeriSign source to confirm the specific implementation of their system. In any event, VeriSign shall not incur any liability by listing this information.

©2009 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, the Checkmark Circle, VeriSign Secured, and other trademarks, service marks and designs are registered or unregistered trademarks of VeriSign, Inc., and its subsidiaries in the United States and foreign countries. All other trademarks are property of their respective owners.

