White Paper

To Increase Downloads, Instill Trust First

Code Signing from Symantec Certifies the Publisher and Integrity of the Code

Symantec™

To Increase Downloads, Instill Trust First

CONTENTS

Building Trust: The First Step to Distributing Software

Whether you develop software for a large company or are a single developer, distributing your software through online and wireless channels brings substantial benefits: You can save money, get your code out faster, and bypass the inventory and fulfillment constraints of shipping out discs and getting space on retailers' shelves. But how can you make best use of those digital channels to circulate your code as widely as possible?

Start by looking at the process of downloading software from your customers' point of view: No matter how exciting your latest application or functionality may be, customers see potential risk in installing your code. Companies and individuals are concerned that they might be putting malware on their computers, smartphones, and other devices, and they have good reason to worry. Malicious code can wreak havoc, stealing personal and financial data, damaging files and systems, compromising confidential information, and more.

Malware also poses a serious threat to the mobile environment, where malicious code can slip into application stores and become a threat to anyone who downloads infected applications. Fixing the damage can cost owners of application stores a significant amount of time and money. Even worse, some damage can't be easily fixed. When application stores lose the trust of their customers, wireless providers and device manufacturers can lose customers, too.

Before potential customers or users can feel comfortable downloading your code—and before most platform and network providers offer it—they need to know two things: First, that an independent third party has verified your identity; and second, that the code hasn't been tampered with since you published it. These two pieces of information give platform providers and end users greater confidence that your code can be trusted.

Code Signing Instills Confidence

Customers feel confident buying software at a brick-and-mortar retail store because shrink-wrapped packaging and mainstream distribution provide third party verification of the publisher and assurance that the software hasn't been tampered with. There is a way to achieve this confidence online as well: by properly signing code.

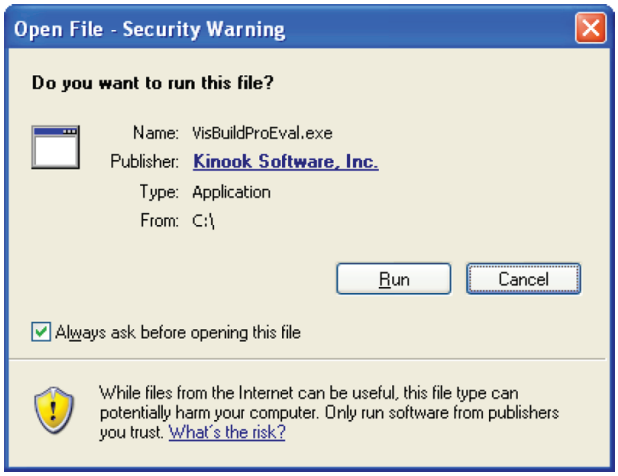
Code signing from a recognized and trusted Certificate Authority (CA) provides explicit third-party confirmation of the publisher's identity. It also helps ensure the integrity of the application since it indicates that code has not been tampered with since the initial digital signature. Just like sealed software purchased at a retail store, code signing can increase customer trust in downloadable applications, and will ultimately help boost your sales and downloads.

Symantec™ Code Signing Certificates help build trust because users see them in action: When users click to download an application, they see a pop-up dialogue box that displays the true identity of the publisher, verified and confirmed by a trusted CA.

By contrast, if the application is unsigned, users will have no information about the publisher and may not feel safe completing the download. If the code is self-signed, they may see an identified publisher but may not trust it anyway, since the publisher is self-identified, instead of identification through a trusted third-party CA. Self-signed code also lacks a trusted root certificate that usually comes preinstalled on most browsers.

Both unsigned and self-signed code can trigger a security alert that the software publisher is unknown and could be detrimental to the system. The more warnings customers see, the less likely they are to commit to downloading the software.

Users know when code comes from a recognized software publisher because they see a dialogue box, similar to this one, which tells them the publisher's identity.



But when code is unsigned, self-signed, or signed by an obscure CA, the system does not recognize the root and displays this warning, which makes it unlikely that users will proceed with downloading and running the application.

Extended validation (EV) Code Signing can help eliminate some of these warning messages. With more secure signing and a more rigorous identity authentication process, EV Code Signing gives reputation services within browsers, operating

system and security software an additional source of confidence in the integrity of applications signed with an EV Code Signing certificate. Microsoft Windows 8 and Internet Explorer 9 and 10 are examples of operating systems and browsers that offer reputation services that recognize EV Code Signing certificates.

How Code Signing Benefits All Software Publishers

As a software publisher or individual developer, the biggest benefit you'll receive from code signing is helping establish trust in your online or mobile applications. Trust stimulates user adoption of digitally shrink-wrapped, code-signed downloadable applications and helps you sell more software online. Also, code signing enables you to respond more rapidly to changing demands and opportunities, accelerating time to market and helping you distribute new applications and updates much faster.

Code signing also protects your intellectual property, making it extremely difficult for criminals to use your company name to distribute counterfeit software or to tamper with your code. If the code is compromised, possibly with malware, the digital signature will not match the original signature and will not be verifiable. This will alert the user that the publisher cannot be confirmed and should not be trusted. This may also free your business of legal responsibility for any damages caused by altered code.

With the reassurance of code signing, platform providers, network providers, and device manufacturers are more likely to accept your applications in their environments, giving you faster, easier access to more channels and more users. Code signing also makes it possible for you to enter partnerships or sales contracts with major companies, increasing your potential market size.

Last, but not least, users are learning to avoid applications that are not signed. Practically speaking, code signing is no longer an option but an essential prerequisite for any company that wants to distribute software online. For example, Microsoft Windows Phone and Windows Azure are among several popular platforms that require all code to be signed before acceptance into their environments.

Best Practices for Code Signing

In conversations with software developers and publishers as well as users, Symantec has developed a variety of code signing best practices:

Give each developer his or her own certificate. Companies often share a certificate among all developers working on the same program, but for security reasons, it is a better idea to issue multiple certificates in order to track the changes made by individual developers.

Sign frequently. Some companies sign code several times a day. That may or may not be necessary, depending on your development procedure, but the majority of companies see value in signing applications at every build.

Code signing is essential to your business because it:

- Eliminates disruptive security alerts that might turn away customers or increase support inquiries
- Helps increase market reach and adoption of downloadable software
- Protects your intellectual property
- Protects your reputation
- Meets the requirements of platforms and network providers
- Builds customer confidence and trust

Make sure your certificates offer time stamping. Time stamping allows users to verify that the code signing certificate was valid when the software was signed, even if the certificate has since lapsed. With time stamping, you won't have to keep renewing certificates on software you're no longer modifying, saving you time and effort while reducing a certificate's total cost of ownership.

Automate the process with Publisher API. If your development process employs continuous build, use the same certificate throughout so that you can keep everything in testing identical to the client experience. Consider Publisher API for daily build or a frequent build cycle.

Use certificates for change control and quality assurance. If you don't use continuous build, designate a production certificate. You can issue self-signed certificates for individual developers that are trusted only on their development computers. When code is ready for production, a manager can sign it with a codesigning certificate that is trusted by the production environment. This way, you can prevent untested code from being installed in your production environment.

Sign all applications for wireless platforms, .NET environments, and kernel mode. Otherwise, it's virtually impossible to distribute them.

Choose a certificate from a leading CA. In a recent survey, developers listed brand reputation and certificate root ubiquity among the most important factors to consider when choosing a code signing solution. With that in mind, it should come as no surprise that seven out of 10 software publishers choose Symantec Code Signing Certificates. Symantec certificates come from the market-leading CA with root certificates preinstalled on most devices and embedded in most applications.[1] If your application is code-signed with a Symantec Code Signing Certificate, almost all platforms will trust it and install it without error messages. Root certificates from smaller CAs are not as likely to be included in the platform, and users may get warning messages.

For new applications, EV Code Signing certificates can help establish reputation. New applications may be flagged as suspicious, even if they are signed, just because they are new and haven't established a reputation. Signing your application with an EV Code Signing certificate, with its more rigorous vetting process and means of signing code, can allow for immediate establishment of reputation, potentially bypassing unknown/unsafe-code warnings in browsers, operating systems, and security software.

Why Choose Symantec Code Signing Certificates

A certificate from a recognized and trusted CA, with an installed trusted root already installed in the browser, will inspire user confidence. A certificate from an unknown CA may generate security warnings and make users suspicious, leading them to check further before they proceed.

1. Online interactive survey of software developers and decision makers, conducted by Symantec, 10/2011.

Choosing Symantec Code Signing Certificates increases the likelihood that users will download your software for two key reasons: ubiquity and broad platform support. Symantec Code Signing Certificates support more desktop and wireless platforms than any other code signing solution while Symantec roots come pre-installed on most platforms and devices. This helps ensure that your Symantec code-signed software will almost certainly install without triggering the security warnings and error messages that can make customers anxious.

Authentication Processes Audited by KPMG

Going beyond the technical aspects, Symantec Code Signing Certificates utilize authentication processes that undergo annual audits by KPMG to confirm the thoroughness of Symantec's approach to identity assurance. Before issuing a certificate, Symantec authenticates that your company is a legally registered organization. In addition, Symantec contacts each signing entity using independently verified contact information to ensure that the registered organization has indeed requested the certificate.

Even individual developers who are not affiliated with an incorporated business can apply for a Symantec Code Signing Certificate. The authentication process is slightly different, yet no less rigorous for individuals.

For Symantec EV Code Signing Certificates, Symantec follows CA/Browser Forum (CABF)-developed guidelines for earning the EV label. These guidelines include an even more stringent vetting process to verify an organization's identity.

Code Signing Certificates

Symantec supports more platforms than any other code signing provider including cloud-based and mobile application platforms. Symantec Code Signing Certificates allow signing of code for Microsoft Authenticode®, Android, Microsoft Office and VBA, Java™, Adobe® AIR™, Qualcomm BREW, Microsoft Windows Phone and Windows Phone Private Enterprise platforms. Once you obtain your certificate, you can sign your code using a signing utility specific to the platform.

With a Symantec Code Signing Certificate, you can sign multiple applications as long as your certificate is active. Each time you sign code, the certificate generates a digital signature using a unique private key that protects the integrity of the code. You sign all code with the same digital signature using public key cryptography (PKI).

When a user's system software or application encounters your signed code, it uses a public key to decrypt the signature. By comparing the hash used to sign the application against the hash on the downloaded application, the system determines whether the code is properly signed. If your code passes this test, most systems will install it without further prompts.

Typically, a code signing certificate is valid for one to three years. However, you can save on the cost of maintaining your code by using the free time-stamping service from Symantec. When code is time stamped, it allows customers to verify that the code signing certificate was valid at the time of the digital signature. Even if the

certificate expires, the signed code is still valid since the certificate was valid when it was signed and time stamped. That's why time stamping is considered a code signing best practice.

Symantec Secure App Service
Symantec also offers a Symantec Secure App Service that makes signing code and managing digital certificates secure, easy and transparent. Symantec Secure App Service is a cloud-based code signing and certificate management solution that helps companies control and secure their code signing activities and keys easily. With Symantec Secure App Service, companies can track vetting and approval of software publishers, code signing activities, key protection and revocation, administrative controls, reporting and audit logs.

Who Requires Code Signing—and Why

Platform providers
Code signing is already a requirement for any program written for the .NET environment, kernel mode, Adobe AIR, Android, and other mobile platform certifications such as Microsoft Windows Apps Marketplace and Symbian Signed.® These platforms will generate warning messages or refuse to install an application unless its code is signed by a recognized Certificate Authority (CA). For instance, every application running on the Android platform must be signed by the developer. Applications that attempt to install without being signed will be rejected either by Google Play or by the package installer on the Android device. Windows platforms such as Azure, Vista, and Server 2008 also require code signing for the Windows Logo program certification. Trends in the industry indicate that soon all operating systems, application development platforms, and mobile devices will only run signed code.

Network providers
Network providers are especially wary of buggy or malicious applications and many of them will not run unsigned code. In a network environment, the potential consequences of downloading malicious code include destruction of the mobile device, service interruption, spread of the malicious application, identity theft, and financial damage. The cost of this damage could run into the billions of dollars within minutes. Not only do network providers fear disruption to service, they also fear any kind of negative experience that might drive away customers. Retaining customers is essential to network providers' business models for sustaining and increasing profitability.

Consumers
Consumers are increasingly cautious about what they download and install on their systems. When they see pop-ups that warn them about possible threats or untrusted publishers, they'll either cancel the installation or call for support. To prevent this issue, code signing serves as a "digital shrink wrap": a way for consumers to benefits from the wider range of choices available through online distribution while getting the same code integrity that they used to get only from physical packages.

Code Signing for Application Stores
If you're considering deploying your applications through third-party application stores, code signing from a recognized CA will likely be a necessary precondition. Code signing helps all parties to an agreement verify that developers have been authenticated and will follow the guidelines for controlling applications. This builds partners' trust in the integrity of your code, so they're likely to deploy those applications more widely and adopt upgrades and new functionality more readily.

Symantec Secure App Service is a flexible solution that meets the needs of developers while eliminating the need for building expensive in-house systems. Symantec Secure App Service also comes with an easy-to-use API that can be seamlessly integrated into the development cycle, automating the process and lifting the burden of manual signing.

For example, organizations or individuals developing and publishing software on the Android platform can use Symantec Secure App Service to protect against lost keys or code. With Symantec Secure App Service, developers can securely manage and track their private keys and applications for increased security and easy application version updates, upload an app image, and access full reporting of signing activity.

For more information about Symantec Secure App Service, please visit: http://go.symantec.com/secure-app-service

Conclusion

Code Signing is Becoming Mandatory for Software Publishers and Individual Developers

Code signing is the best way to meet the requirements of today's code transfer environment, which demands publisher/developer verification and proof of code integrity. By certifying the origin of the code and guarding against unauthorized code changes, code signing creates a digital "shrink-wrap" for code that builds the confidence of users, platform providers, network providers, and device manufacturers. Code signing is a win-win—protecting your business reputation also protects your buyers and users, which in turn increases adoption of your downloadable software.

Symantec Code Signing Certificates are the best choice for code signing solutions because they support more platforms than any other code signing certificate provider. In addition, Symantec™ root certificates are embedded in more applications and preinstalled on more devices than any other CA. With a Symantec Code Signing Certificate authenticating your code, users are more likely to download it and their systems are likely to install it without question. And once your certificate has helped you establish user trust, you have the chance you've been looking for: To impress customers and users with the innovation and functionality of your software, increase sales and distribution, and grow your business.

More Information

In United States or Canada

Visit our website

http://go.symantec.com/code-signing

To speak with a Product Specialist, please call or email

1 (866) 893-6565 or 1 (520) 477 3135 codesigning@symantec.com

In Europe, Middle East or Africa (EMEA)

Visit our website

http://www.symantec.com/en/uk/code-signing

To speak with a Product Specialist, please call or email:

United Kingdom and Ireland +0800 032 2101 Rest of EMEA +353 1 793 9053

United Kingdom talk2us-uk@symantec.com Rest of EMEA talk2us-ch@symantec.com

In Asia-Pacific

Visit our website

http://www.symantec.com/en/aa/code-signing

To speak with a Product Specialist, please call or email:

Australia	+61 3 9674 5500
New Zealand	+64 9912 7201
Hong Kong	+852 30 114 683
Singapore	+65 6622 1638
Taiwan	+886 2 2162 1992

Taiwan, Hong Kong, Singapore	ssl_sales_asia@symantec.com
Australia, New Zealand	ssl_sales_au@symantec.com

To speak with additional Product Specialists outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec protects the world's information and is the global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device to the enterprise data center to cloud-based systems. Our industry-leading expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at: go.symantec.com/socialmedia.

Symantec World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
1-866-893-6565
www.symantec.com

UID:223/07/14