

Understanding Code Signing & the Code Signing Channel Opportunity

Expanding market reach by distributing trustworthy software over the Internet

GLOBALSIGN WHITE PAPER

Version 1.3



www.globalsign.com

CONTENTS

Contents	2
Introduction	3
Code Signing	3
Why and when to sign code	4
What Platforms Support Code Signing?	4
Self sign vs. public root	4
The Benefits of Signing Code with a GlobalSign Code Signing Certificate	5
Buyer considerations	6
Code Signing for VARs and ISV Partners	6
Resources	7
About GlobalSign	7

INTRODUCTION

As Operating System and Browser vendors like Microsoft, Apple, Mozilla, Ubuntu and others move towards higher security models for executable application privileges and lock down capabilities on “unknown” code, being able to identify legitimate applications from “bad” applications (badware) becomes increasingly important for both users and developers. One method of making applications/code stand out from the increasing masses of badware is to employ digital signatures, commonly referred to as “Code Signing”. This White Paper examines the basics of why and how to Code Sign applications, the benefits it provides developers who employ its use, the platforms supporting the Code Signing model, and finally the financial opportunity for reselling GlobalSign Code Signing to VARs operating direct, or indirect, relationships with developers and software vendors.

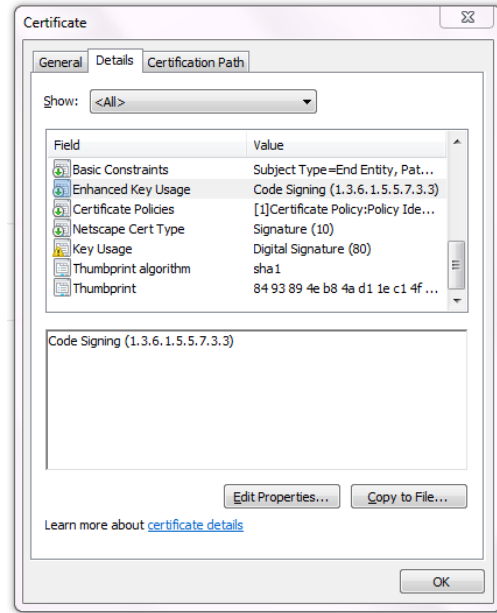
CODE SIGNING

Code signing (or object / application signing) is the virtual equivalent to shrink-wrapping CD based software for distribution. With Code Signing, the end user knows the digitally signed software being executed on their Windows machine is legitimate, comes from a known software vendor and the code has not been tampered with since being published. In essence, code signing using a trusted third party like GlobalSign prevents:

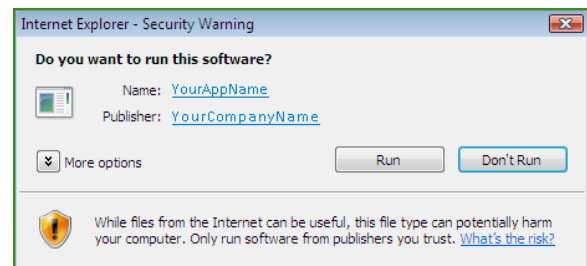
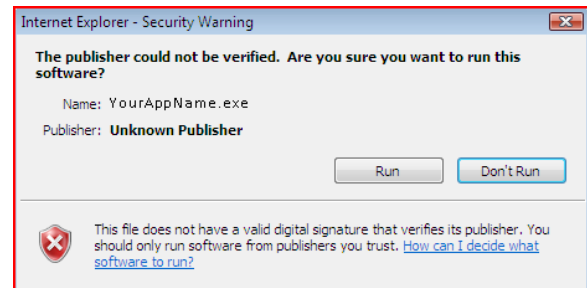
- **Users abandoning the installation of an application that is not easily identified as genuine**
- **Malicious alteration of legitimate code**
- **Identity theft of vendor or code author**

Therefore, any Windows developer should seriously consider implementing instantly recognizable digital signatures as a way to enhance consumer confidence.

Software developers digitally sign code or software distributed over the Internet using X.509 v3 Digital Certificates marked for the specific use of digitally signing code. In Public Key Infrastructure (PKI) this is referred to as Key Usage. Below displays an example of a GlobalSign Digital Certificate marked for code signing (Code Signing Certificate).



The two User Interface (UI) images below depict the end user experience when installing code via Internet Explorer. In the first instance, the code has not been digitally signed by a Certificate issued from a trusted Certificate Authority, and therefore presents the end user with a warning message that may cause them to abandon the install.



Conversely, the second image presents the publisher's identity: shown via a link to more identity details from the Certificate.

Code Signing allows developers to include information about themselves and their code through the use of digital signatures. To create a digital signature (the act of Code Signing) the developer must use a Digital Certificate. The Digital Certificate binds the identity of a person or entity to a public key that is mathematically related to a corresponding private key pair. The private key must be vigorously protected and in some cases may represent the electronic equivalent of a "wet ink" signature when associated with a Digital Certificate. The private key is used to apply a digital signature to a shortened version of the code that is run through a hashing algorithm and the public key is used to verify the signature. Many applications require code to be signed prior to distribution. Signing the hash of the code with an algorithm like RSA SHA1 provides a method to validate if the code has changed in any way since it was signed. Even changing one character in a line of code will alter the hash and be detected as suspect. If you plan on deploying an application that uses any active content, such as device drivers, ActiveX controls or macros you should become familiar with the digital signing requirements well in advance of your planned launch date.

WHY AND WHEN TO SIGN CODE

Although networks like the Internet provide tremendous market reach for developers to distribute their applications, recipients of delivered applications over these networks are not provided the same types of assurance they would have if the software were obtained through traditional "shrink wrap" methods found at their local retail store. Unlike store purchased software, tamper evident packaging doesn't exist; there is no trusted visible supplier to stand behind the transaction, and there is no obvious way to determine where the software originated. Microsoft recognizes the need of users who depend on applications to be reliable and malware-free and therefore require an increasing number of applications to be digitally signed. In summary, signing your code is good for users downloading applications, and good for developers as an increase in trusted ecommerce translates into increase in downloadable software.

WHAT PLATFORMS SUPPORT CODE SIGNING?

Different software platforms have different requirements and different options available for digitally signing code. GlobalSign's Code Signing Certificates supports the following platforms:



Microsoft Authenticode - Windows ActiveX controls can be signed via Authenticode (32 bit and 64 bit .exe, .ocx, .dll or other) and Kernel software for Windows. Windows 7 compatible*.



Adobe AIR applications – Adobe AIR only allows digitally signed applications to be run.



Java - JAR applet files can be signed to allow apps access to client-side resources.



Microsoft Office & VBA – Digitally sign Microsoft Office macros and Visual Basic Applications (VBA) to avoid Unknown Publisher macro warnings.



Apple Mac applications - code signing was introduced by Apple in MacOS 9 onwards.



Mozilla & Netscape Objects - Digitally sign Mozilla and legacy Netscape Object files to enable activation in Mozilla browsers.

** Only select Certificate Authorities are enabled by Microsoft to allow Windows Kernel 64 bit code signing. GlobalSign is one such Certificate Authority – please check with your choice of vendor if you plan on using an alternative to GlobalSign to sign 64 bit Windows applications*

SELF SIGN VS. PUBLIC ROOT

There are two basic types of Code Signing Certificates that can be used to sign applications:

- **Self-Signed Code Signing Certificates**
- **Public Root Code Signing Certificates**

Self-signed Code Signing Certificates are effectively untrusted credentials that relying parties have no immediate way of verifying the authenticity of the publisher. The sole benefit of signing code with a self-signed Certificate surrounds the hashing technology that is used to verify if the code has been altered subsequent to signing. The downside of signing with a self-signed Certificate is the recipient of the code has no obvious way of knowing if the identity is authentic. Self-signed Code Signing Certificates are typically best suited for signing test code.

Alternatively, public rooted Code Signing Certificates, like those from GlobalSign, provide not only a mechanism to assure the integrity of the software content, but also a method to instantly verify the origins of the software. As a web-trusted Certificate Authority, GlobalSign “vets” both the publisher and publisher’s organization in accordance with the strict guidelines outlined in the GlobalSign Certificate Practice Statement (CPS).

www.globalsign.com/repository.

The CPS is mainly for the benefit of the party who relies on the Certificate as a full representation of the individual and organization that it identified. The binding of an identity to published code provides the accountability all involved in the transaction require for a trusted transaction to occur. The recipient of the downloaded code has an independent third party verification of the publisher, and the publisher has greater assurance malicious code or malware won’t be published by individuals masquerading as them.

THE BENEFITS OF SIGNING CODE WITH A GLOBALSIGN CODE SIGNING CERTIFICATE

- **Removes the "Unknown Publisher" popup in Operating Systems and browsers**
- **Full timestamping service included free of charge – timestamping code ensures the signature does not expire**
- **Allows an unlimited number of applications to be signed within the lifespan of the certificate**
- **Supports all developer platforms**
- **Offers multi-year savings - plus multi-year avoids having to renew annually**
- **Offers a risk free refund**
- **Comes with a \$100,000 Warranty - underwritten Liability program**
- **Multi-Language Tech Support - access to expert technical support staff via email & telephone**
- **Issued by an organization that’s been a WebTrust Accredited Certification Authority since 2002**

BUYER CONSIDERATIONS

If you decide to obtain a publicly trusted Code Signing Certificate, then you probably already know you have a choice of Certificate Authority to buy from. You should take the following areas into consideration when selecting:

Ubiquity	Is the root authority that the Code Signing Certificate is issued from trusted in the application platform? Also, are the recipients of your application going to automatically trust the signature applied to the code? The answer can only be “yes” if the Authority has a global root embedment program to ensure that all applications and operating systems are supported.
Timestamping services	It is best to make sure signatures do not become invalid after the Certificate expires.
Price and Value	Am I getting good value for the experience, support, and functionality when compared to the price?
Support	Am I working with a supplier whose core business is Digital Certificates?
Trust	What types of third party independent audits, such as WebTrust, verify the Authority is operating in full compliance with their published Certificate Practice Statement (CPS). Is the Authority well respected and credible in the industry? Do they have a good reputation – as a good reputation of the Authority can inspire additional downloads of your applications.
Support for Individuals AND Commercial Software Publishers	Software publishers are grouped into one of two categories – individuals who publish their own software and commercial software publishers. Make sure your choice of Authority supports your category. Many Authorities only support commercial software publishers and not individuals.

CODE SIGNING FOR VARS AND ISV PARTNERS

In competitive times, VARs are looking for value-add products that complement core services and existing portfolios. If your organization is involved in the value or supply chain for developing, testing, deploying or distributing software over the Internet, you have the opportunity to add a new revenue line and maximize customer satisfaction by offering Code Signing Certificates as part of your core service.

GlobalSign has a SaaS (Software as a Service) web portal designed to make the application of Code Signing Certificates by VARs and Partners quick and easy. GlobalSign conducts all the necessary vetting and can send the issued Certificate to either the Partner, or the end Developer. The Certificate is issued in the developer’s name to ensure the right identity is associated with the digitally signed code. Alternatively, a flexible XML API will allow the process to be automated and integrated into your own workflows.

Code Signing Certificates from VeriSign are approximately \$500 per annum. GlobalSign offers a cost effective alternative that supports both corporate identities and individual developer identities for \$229, and offers exceptional multi-year discounts. Partners receive instant discounts, and no commitment for buying inventory is needed. Just apply for Certificates on behalf of customers as and when they are needed or host a reseller specific customer ordering URL where the developer can initiate the order directly from your site. . Alternatively for larger VARs, a deposit/bulk purchase model offers highest discounts on Code Signing Certificates available today.

Partners may use their GlobalSign Partner Account to resell all GlobalSign Digital Certificate solutions including:

- **Code Signing Certificates**
- **SSL Certificates**
- **Email Encryption (S/MIME) Digital IDs**
- **Adobe Certified Document Services (CDS) Digital IDs**

RESOURCES

For further information, data sheets, guides, pricing, and FAQs on GlobalSign code signing products, or to buy individual Code Signing Certificates please go to:
www.globalsign.com/code-signing.

Contact the GlobalSign Partner Team at www.globalsign.com/company/contact.html to discuss the Code Signing opportunity for VARs and ISV supply chain Partners.

ABOUT GLOBALSIGN

GlobalSign was one of the first Certification Authorities and has been providing digital credentialing services since 1996. It operates multi-lingual sales and technical support offices in London, Brussels, Boston, Tokyo and Shanghai.

GlobalSign has a rich history of investors, including ING Bank and Vodafone. Now part of a GMO Internet Inc group company - a public company quoted on the prestigious Tokyo Stock Exchange (TSE: 9449) whose shareholders include Yahoo! Japan, Morgan Stanley and Credit Suisse First Boston.

As a leader in public trust services, GlobalSign Certificates are trusted by all popular Browsers, Operating Systems, Devices and Applications and include SSL, Code Signing, Adobe CDS Digital IDs, Email & Authentication, Enterprise Digital Solutions, internal PKI & Microsoft Certificate Service root signing. It's trusted root CA Certificates are recognized by all operating systems, all major web browsers, web servers, email clients and Internet applications; as well as all mobile devices.

Accredited to the highest standards

As a WebTrust accredited public Certificate Authority, our core solutions allow our thousands of enterprise customers to conduct secure online transactions and data submission, and provide tamper-proof distributable code as well as being able to bind identities to Digital Certificates for S/MIME email encryption and remote two factor authentication, such as SSL VPNs.

GlobalSign Inc	GlobalSign NV	GlobalSign Ltd
Toll Free: 1-877-SSLGLOBAL	Tel: +32 16 891900	Tel: +44 1622 766766
Fax: 603-570-7059	Fax: +32 16 891909	Fax: +44 1622 662255
www.globalsign.com	www.globalsign.eu	www.globalsign.co.uk
sales@globalsign.com	sales@globalsign.com	sales@globalsign.com
