An Introduction to

CODE SIGNING

GlobalSign®

CONTENTS.

Chapter 1.

What is Code Signing

WHAT IS CODE SIGNING

Code Signing is the virtual equivalent to shrink wrapping CD based software for distribution.

Customers who buy software from a retail store receive a shrink-wrapped package and can clearly determine who published the software and whether or not the package has been tampered with or opened. Therefore, the customer can easily make a decision whether or not to trust the software. Customers, who download software from the internet, need similar assurance. Code Signing provides this assurance and acts as a "virtual shrink wrap" when distributing Software via the internet.

Code Signing is the process of applying a digital signature to software/applications distributed over the Internet. Signed code provides customers the same security as store bought, shrink-wrapped software as once the code is signed it includes the name of the publisher and protects against malware injections and other corruptions.

Code Signing proves the "signed" software is:

- Legitimate
- Comes from a known software vendor
- Code has not been tampered with since being published

Code Signing prevents:

- Users abandoning the installation of an application
- Malicious alteration of legitimate code
- Identity theft of vendor or code author

Chapter 2.

Code Signing Certificates 101

What is a Code Signing Certificate?

Code Signing Certificate Defined

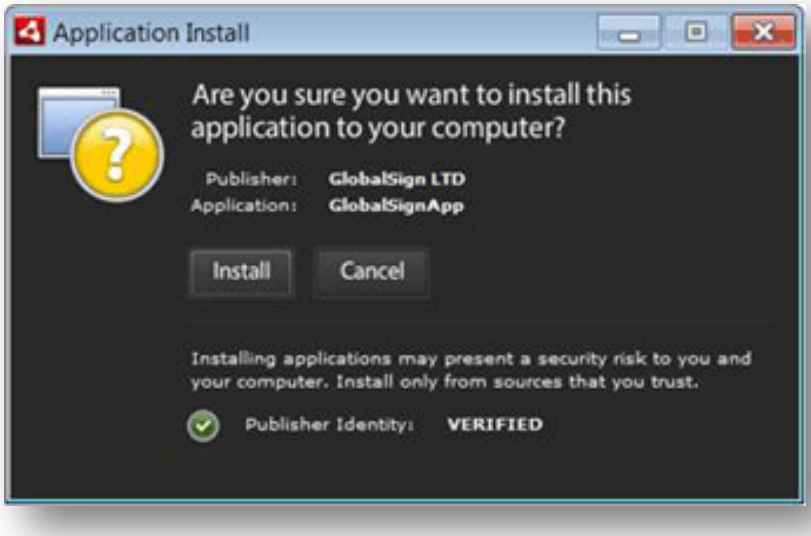
A Code Signing Certificate is a Digital Certificate that contains information that fully identifies an entity and is issued by a Certificate Authority such as GlobalSign.

A Code Signing Certificate 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 uses a Digital Certificate.

The Digital Certificate binds the identity of an organization to a public key that is mathematically related to a corresponding private key pair. 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. Signing the hash of the code 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.

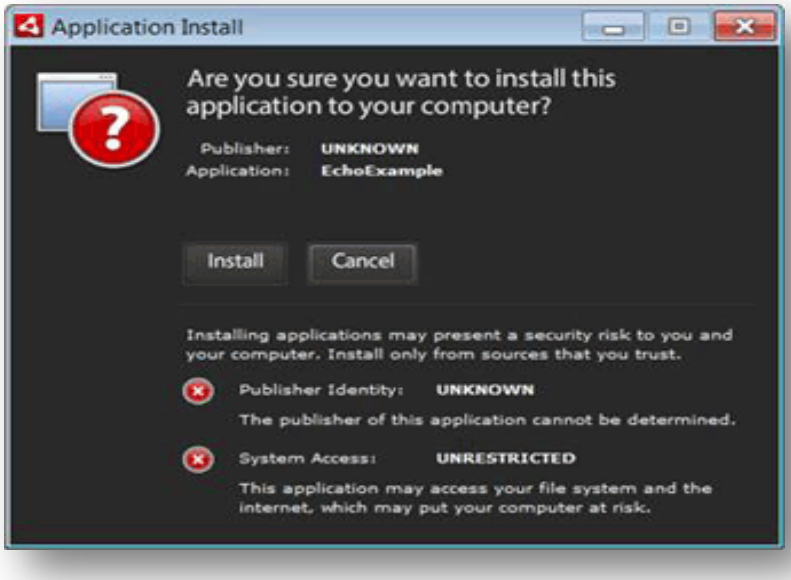
Code Signing Certificates in Action

Application Signed with a Code Signing Certificate



Digitally signed applications prominently display the name of the publisher on the install screen, confirming the application is verifiable and from a trusted source.

Application NOT Signed with a Code Signing Certificate



Unsigned applications display worrying security alerts to end users, warning them that the publisher of the application is unknown and advising them to only install applications from sources that they trust.

Code Signing helps prove:

Content Source

Code Signing identifies that the software or application is coming from a specific source (a developer or signer). When software is downloaded from the internet, browsers will exhibit a warning message stating the possible dangers of downloading data, or display an "unknown publisher" warning. Code Signing **removes the "Unknown Publisher" security warnings** and identifies the Publisher's name (ie. Organization Name).

Content Integrity

Code Signing ensures that a piece of code has not been altered and determines whether code is trustworthy for a specific purpose. If the application/ software code is tampered with or altered after digitally signing, the signature will appear invalid and untrusted.

Signed code is beneficial for users downloading applications and beneficial for developers. Users are assured who they are downloading software from and can decide whether or not to trust the source. Developers can mark their "brand" and protect their software from unwanted changes.

Chapter 3.

Why and When to Digitally Sign Code

Why and when you should Digitally Sign Code

Running unsigned code can be dangerous!

Unlike store purchased software, tamper evident packaging doesn't exist for online software; there is no trusted visible supplier to stand behind the transaction, and there is no obvious way to determine where the software originated.

Unsigned software is subject to tampering, such as the insertion of spyware or malware, so end users are encouraged not to run unsigned code. Because of this downloading or running unsigned applications will generate worrying "Unknown Publisher" security warnings.

Distributing software enables developers to deliver brand rich internet applications on the desktop resulting in a closer connection with the customer. This boost the productivity and functionality of web applications translating to greater reach of web servers and enhanced customer experience.

Code Signing encouraged by platform providers

Various platforms support code signing allowing you to sign different types of code.

Microsoft Authenticode

Sign .exe, .cab, .dll, .ocx, .msi, xpi, .xap, ActiveX controls and Kernel software

Adobe Air

Sign .air and .airi files

Apple

Sign software, applications, plug-ins and content for Mac OS desktops

Mozilla & Netscape

Sign Mozilla XPI packages for Firefox and files for Netscape Objects

Macros and Visual Basic Applications

Sign VBA objects, scripts and macros within Microsoft Office

Java

Sign .jar files and Java applications

Chapter 4.

Self-Sign VS. Publicly Trusted Signatures

Self Signed VS. Publicly Trusted Signing

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

Self-Signed Code Signing Certificates are essentially untrusted credentials where relying parties have no immediate way of verifying the authenticity of the publisher

Considerations for using a Self-signed Certificate:

•Recipient of the code has no obvious way of knowing if the identity is authentic

•Signatures will display a trust warning indicating that the publisher is unverified and will display “Unknown Publisher”

•Self-signed certificates cannot be revoked, so if the certificate is compromised it could harm the users of your software

Self-signed Code Signing Certificates are typically best suited for signing test code.

.

Self Signed VS. Publicly Trusted Signing

Publicly Trusted Code Signing Certificates

Publicly trusted Code Signing Certificates are certificates that are issued from a publicly trusted Certificate Authority (CA).

Public rooted Code Signing Certificates, like those from GlobalSign, provide not only a mechanism to assure the integrity to 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.

Benefits of using a Publicly Trusted Code Signing Certificate:

Digitally signing your code with a Code Signing Certificate issued from a publicly trusted CA provides many benefits including:

- Displays publishers name when recipient is downloading signed application
- Certificates can be revoked if a certificate becomes compromised.
- Code is digitally signed with a time stamp

Time Stamping

It's important to understand the benefit of time stamping because it extends the trust of the code. When a digital signature is applied, a timestamp is also recorded. This time stamping feature acts to ensure the signed code remains valid even after the digital certificate expires. Unless you're adding additional code to your application, a new signature will not need to be applied even if the Certificate used to initially sign the code expires.

Chapter 5.

Buyer Considerations

Buyer considerations

If you decide to purchase a Code Signing Certificate from a publicly trusted Certificate Authority, then you probably have several CA choices available to purchase from. You should take the following areas into consideration when selecting a code signing provider:

Ubiquity

For the recipients of your application to trust the signature applied to the code the CA needs to have a global root embedment program to ensure that all applications are supported.

Time Stamping Services

To ensure the signature doesn't become invalid after the digital certificate expires consider choosing a Certificate Authority that offers free time stamping service.

Price and value

Are you getting a good value for the experience, support and functionality when compared to the price

Support

Are you working with a supplier whose core business involves digital certificates

Signature Volume Limits

Is there a limit to the number of signings one can apply using the digital ID

Trustworthiness

What types of third party independent audits such as WebTrust, verify the Certificate Authority is operating in full compliance with their published Certificate Practice Statement

Ease of Use

How easy is it to apply the certificate; how easy is it to install

Build trust and show users your code is from a trusted developer

GlobalSign Code Signing Certificates are multi-purpose meaning you can digitally sign multiple platforms using a single certificate. One Certificate can be used to digitally sign:

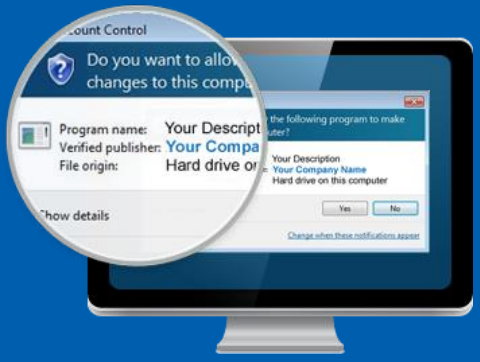
- Microsoft Authenticode files (32 and 64bit) including Kernel software
- Adobe Air Applications
- Apple Desktop Applications
- Java applications
- Microsoft Office Macros and Visual Basic
- Mozilla XPI packages for Firefox

Other unique GlobalSign Code Signing features:

- Digitally sign an unlimited number of applications
- Time stamping service included enables the digital signature to not expire
- Free Code Signing Tool available to simplify the signing process.

"What makes significant difference to other certificate providers is that we have been able to sign both user and kernel-space code with the same certificate.

The code-signing tool provided makes things really easy, but whenever help was required, we have found the GlobalSign people right on our side, every step of the way, with really immediate and personal communication."
Nikos Mouratidis, Qualtek.



BUY A CODE SIGNING CERTIFICATE TODAY!

www.globalsign.com/code-signing/

GlobalSign