



GlobalSign Digital IDs for Adobe AIR Code Signing

Expanding market reach by distributing trustworthy software over the Internet

WHITE PAPER

Lila Kee – Director of Business Development, GlobalSign Inc

TABLE OF CONTENTS

| | | |
|----|---|----------|
| 1. | CODESIGNING DEFINED..... | 3 |
| 2. | WHY AND WHEN SHOULD ONE SIGN CODE..... | 4 |
| 3. | SELF SIGN VERSUS PUBLICLY ROOTED SIGNATURES..... | 4 |
| 4. | HOW IT WORKS:..... | 6 |
| 5. | BUYER CONSIDERATIONS..... | 7 |
| 6. | ABOUT GLOBALSIGN..... | 7 |
| 7. | RESOURCES..... | 8 |

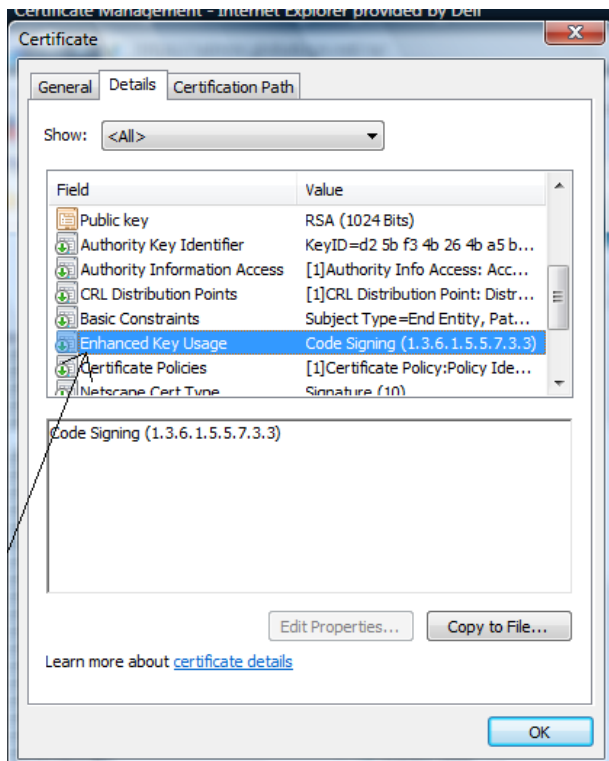
1. CODE SIGNING DEFINED

Code signing or sometimes referred to as object signing is the virtual equivalent to shrink-wrapping CD based software for distribution. With GlobalSign Code signing for Adobe AIR, the end user knows the digitally signed software 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:

- **The strong possibility of users abandoning the installation of an application that is not easily identified as genuine**
- **Malicious alteration of legitimate code**

Identity theft of authorship Therefore, any Adobe Air developer or organization distributing applications over the internet or intranet should seriously consider implementing instantly recognizable digital signatures as a way to enhance consumer confidence.

Software vendors and developers can digitally code sign the software they distribute over the Internet using X.509 v3 digital IDs marked for the specific use of digital signing code. In the world of Public Key Infrastructure (PKI) this is referred to as Key usage. An example of GlobalSign digital ID marked for code signing.



Digital IDs a.k.a. Digital Certificates, bind the identity of a person or entity to a public key that is mathematically related to a corresponding private key pair often generated using standard browser technology. 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 ID. The private key is used to apply a 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 including those developed on the Adobe AIR platform 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 a one character change will alter the hash and therefore be detected as suspect. If you plan on shipping an Adobe AIR application you

should become familiar with the digital signing requirements well in advance of your planned ship date since the Adobe AIR installer will require you to digitally sign your application in order to make it installable by users.

2. WHY AND WHEN SHOULD ONE SIGN CODE

Although unsecure 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. Distributing software on platforms like Adobe AIR enables developers to deliver branded rich internet applications (RIA) on the desktop resulting in a closer connection with the customer. This boosts the productivity and functionality of web applications translating into greater reach of web services and enhanced customer experience. Since RIAs deployed on Adobe AIR provide deeper integration to the desktop than browser based applications, assurances that the application and its developer are legitimate become essential to the end user. Adobe AIR recognizes the need of users who depend on applications to expect reliable and free of malicious-ware and therefore require applications to be digitally signed. Because AIR only permits digitally signed applications to be installed, the digital signature assures users a method to identify which developer signed a particular application providing assurances that the application is legitimate. In summary, signing your code is good for users downloading applications running on Adobe AIR, and good for developers as an increase in trusted ecommerce translates into increase in downloadable software.

3. SELF SIGN VERSUS PUBLICLY ROOTED SIGNATURES

There are two basic types of digital IDs that can be used to sign applications on Adobe AIR:

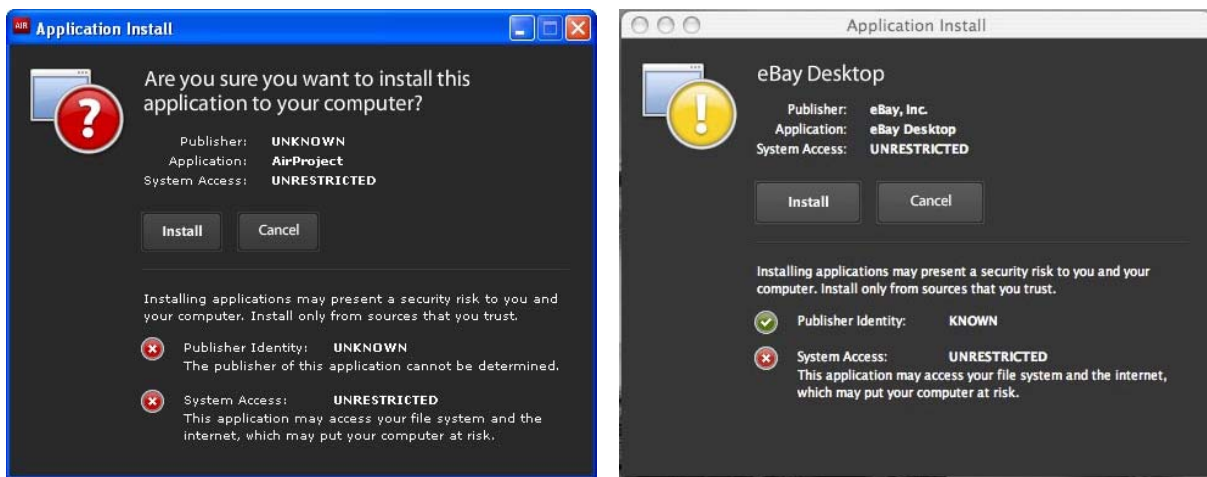
1. **Self Signed Digital IDs**
2. **Publically Root Digital IDs**

Self signed digital IDs are effectively un-trusted credentials that relying parties have no immediate way of verifying the authenticity of the publisher. About the sole benefit of signing code with a self-signed digital ID 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 digital ID is the recipient of the code has no obvious way of knowing if the identity is authentic. Self signed digital IDs are typically best suited for signing test code.

Alternatively, public rooted digital IDs, like those from GlobalSign, provide not just 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). <http://www.globalsign.com/repository/index.htm>. The CPS is mainly for the benefit of the party who relies on the digital ID 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 won't be published by individuals masquerading as them.

These two User Interface (UI) images depict the end user experience when installing code running on Adobe AIR. In the first instance, the code has been signed using a non verifiable self signed digital ID, and therefore presents the end user with a warning message that may cause them to abandon the download.



Source: http://www.adobe.com/devnet/air/articles/signing_air_applications_07.html

Conversely, the second image depicts a trusted symbol presented to the user because the publisher's identity is known.

It's important to note, unless you utilize the ADT migrate command, your AIR application can only be updated using a digital signature from the same digital ID used to sign the initial application. Therefore, developers should take caution when considering shifting from a self signed digital ID to a publically trusted one. (or from switching from one publically trusted digital ID to another provided by a different Certificate Authority.)

4. HOW IT WORKS:

The following provides a high-level walk through showing how to enroll for and use a GlobalSign code signing digital ID to sign code for Adobe AIR. Detailed guides are referenced in the resource section found later in this document.

1. Visit the GlobalSign website <http://www.globalsign.com/developer/code-signing-certificate/index.htm> and select Code Signing Certificate – Object Signing. For Adobe AIR Digital IDs, you must enroll using the Firefox browser.
2. Select the Adobe AIR code signing type, the digital ID validity (Digital IDs can be purchased with 1, 2 & 3 year validities) and complete the enrollment form by entering the required information about you and your organization.
3. Your Firefox browser will then create a Certificate Signing Request (CSR) that will contain a public key that corresponds to the private key stored on your computer. This CSR will be sent to GlobalSign for subsequent signing by the GlobalSign public root hierarchy.
4. Fax identity verification documentation to the GlobalSign vetting team. They will use this information to verify the authenticity of the subscriber based on the Certificate Practice Statement (CPS) guidelines.
5. Subsequent to identity verification, you will receive an email that includes a “pick up” URL that will allow you to install your digital ID. Remember you must pick up your digital ID on the same computer as the one used to initiate the request.
6. Since the Adobe signing tools can't directly access the Firefox keystore, you'll have to export both your keys and the certificate into a PKCS12-based keystore file. See GlobalSign FAQs for detailed instructions on how this is accomplished. And because GlobalSign Code Signing digital IDs are issued from an intermediate CA that is “chained” to the GlobalSign trusted root, you will need to also make sure you include the intermediate CA prior to signing your code.
7. As a best practice, GlobalSign strongly recommends you protect your private key by establishing a minimum password. If your private key becomes lost or stolen, you must report the compromise immediately to GlobalSign in order for the digital ID to be revoked. Revocation will help prevent others from publishing code in the future under your identity.

You are now ready to prepare your .air or .airi (developers affiliated with large organizations may need to produce an AIR Intermediate package – AIRI or .airi file for later signing by someone authorized to bind the organization to the application) to be digitally signed with your GlobalSign issued code signing for Adobe AIR digital ID. Please consult Adobe documentation for platform specific guidelines on how to use your code signing digital ID to sign your code:

- *Dreamweaver CS3*: www.adobe.com/go/learn_dw_air_signature_en
- *Flex3 SDK*: www.adobe.com/go/learn_flexsdk_air_signature_en
- *Flex Builder 3*: www.adobe.com/go/learn_flexbuilder_air_signature_en

- *Flash CS3 Professional*: www.adobe.com/go/learn_flash_air_signature_en
- *AIR SDK*: www.adobe.com/go/learn_airsdk_air_signature_en

Timestamping: GlobalSign provides time-stamping services to ensure the signed code remain valid even after the digital ID expires. Unless you're adding additional code to your application, a new signature will not need to be applied even if the digital ID used to initially sign the code expires.

5. BUYER CONSIDERATIONS

If you decide to go the public digital ID route, 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** – Is the root authority that the digital ID is issued from trusted in the platform?
- **Timestamping services** – It is best to make sure signatures don't become invalid after the digital ID expires.
- **Ease of use** – How easy is it to apply for the digital ID; how easy is it to install?
- **Price and value** - Am I getting good value for the experience, support, and functionality when compared to the price.
- **Signature volume limits** - Is there a limit to the number of signings one can apply using the digital ID?
- **Support** - Am I working with a supplier whose core business involve digital certificates?
- **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 (CPS).

6. ABOUT GLOBALSIGN

GlobalSign has been securing identities, websites and transactions, worldwide, for more than 10 years. GlobalSign has a rich history of investors, including ING Bank and Vodafone. In October 2006 GlobalSign became part of the GMO Internet, Inc. (TSE: 9449) group of companies. Immediately a newly appointed Management Team was formed – comprising of a number of industry veterans with experience of establishing operations and creating successful market positions for Certificate Authorities like GeoTrust, CyberTrust and Comodo. Offering the most feature rich and highly valued SSL Certificates available in the industry GlobalSign is ready to take our existing and new corporate customers to the next level of managed security solutions.

GlobalSign is a highly credible and well established [Certificate Authority](#) (CA) and [SSL](#) Provider. A leader in public trust services GlobalSign has been issuing trusted [digital certificates](#) since 1996 – delivering its Public Trust from a highly ubiquitous trusted public root.

In 1998, GlobalSign had the foresight to create a strong Root Certificate by using 2048 bit RSA keys. This makes GlobalSign the only Certification Authority to have a widely embedded Root Certificate that

meets the NIST (National Institute of Standards & Technology) recommendation that from 2011 onwards all cryptographic keys should be 2048 bit in strength.

The GlobalSign trusted roots are recognized by all operating systems, all major web browsers, web servers, email clients, internet applications and devices that require [SSL Certificates](#). Investors such as Vodafone have helped make it possible for GlobalSign to become an expert in providing trusted certificates and secure mobile technology to cellular devices and mobile phones.

Our Root Ubiquity summary is available here:

https://www.globalsign.com/resources/ssl_root_compatibility.pdf

7. RESOURCES

For product descriptions, data sheets, guides, pricings, and FAQs on GlobalSign code signing products please go to: <http://www.globalsign.com/developer/code-signing-certificate/index.htm> or contact GlobalSign Sales by contacting us at https://www.globalsign.com/contact/form_en.html.

GlobalSign Inc
2 International Drive
Suite 330, Portsmouth
New Hampshire 03801
Toll Free: 1-877-SSLGLOBAL
Fax: 603-570-7059
www.globalsign.com
sales@globalsign.com

GlobalSign NV
UbiCenter, Philipssite 5
3001 Leuven
Belgium
Tel: +32 16 891900
Fax: +32 16 891909
<http://eu.globalsign.com>
sales@globalsign.com

GlobalSign Ltd
Springfield House
Sandling Road, Maidstone,
ME14 2LP, United Kingdom
Tel: +44 1622 766766
Fax: +44 1622 662255
<http://www.globalsign.co.uk>
sales@globalsign.com

