



BUSINESS GUIDE

SECURING YOUR SOFTWARE FOR THE MOBILE APPLICATION MARKET

THE LATEST CODE SIGNING
TECHNOLOGY



CONTENTS

- 1 THE CHALLENGE
 - 1 A BRIEF REVIEW OF CODE SIGNING
 - 2 THE SOLUTION
 - 2 HOW THE CODE SIGNING PORTAL WORKS
 - 3 SUPPORTED PLATFORMS
 - 3 THE BENEFITS
- 3 SUMMARY



SECURING YOUR SOFTWARE FOR THE MOBILE APPLICATION MARKET

THE LATEST CODE SIGNING TECHNOLOGY

THE CHALLENGE

Thanks to recent innovations in the mobile device industry, demand for mobile applications has soared. In fact, consumers have already downloaded billions of applications for mobile devices, and industry reports point to ongoing rapid growth in the mobile apps market¹.

At the same time, malware continues to infect sites at an explosive rate. According to recent research, the number of sites with malicious code increased by over 800 percent within a single year and cybercrime is now estimated to cost businesses more than \$100 billion annually². The proliferation of mobile applications—and the growing threat posed by malware—mean that mobile devices and networks now face an even greater risk of becoming infected with malicious content. Once an infection occurs, the consequences can be potentially disastrous for consumers, developers, and network operators alike.

Mobile application developers need to secure their code and content to protect the integrity of their software and the reputation of their business. Similarly, consumers need assurances that the latest cool game or productivity application that they are downloading to their mobile device is coming from a trusted source and has not been tampered with during transit. At the same time, legitimate independent software vendors (ISVs) who typically publish multiple applications—and several versions of each application—need easy-to-use tools to track and administer their software. Tools, such as a web-based management portal, can track releases and safely “recall” specific versions that become infected without impacting the rest of their published applications.

In this business guide, we discuss how the latest Code Signing technology works to secure software code and content for applications that are directly downloaded onto mobile devices from the Internet. These applications can come either from the software publisher’s or application reseller’s web sites, or

directly from the mobile service provider’s network. We will also show why Code Signing platforms need to be flexible, scalable, user-friendly, and easily adaptable to different mobile operating platforms.

A BRIEF REVIEW OF CODE SIGNING

Code Signing digital certificates (certs) have been used for many years to sign and digitally “shrink wrap” executable software such as software objects, firmware images, Java applications, device drivers, and Microsoft Visual Basic® for Applications (VBA) macros. They have also been used for static content, such as virus updates, configuration files or documents, and other forms of content that are transmitted over the Internet where the end user does not know the content publisher.

In order to protect the end user from malicious content and offer authentic software vendors and content publishers a way to establish trust with their end customer, Certificate Authorities (CA) such as VeriSign employ a Public Key Infrastructure (PKI) methodology.

Briefly, PKI encompasses the hardware, software, policies, and procedures needed to create, manage, distribute, and revoke digital certificates. With PKI, data is encrypted using asymmetric public and private keys, where the private key is kept secret and the public key is digitally signed by a third party known as a Certificate Authority (CA) and may be widely shared. In Code Signing, software developers use their private keys to encrypt a digital signature. When end users decrypt the signature with the corresponding public key, it confirms the publisher’s identity and the integrity of the code.

Code Signing technology has evolved to include several standard features, including a PKI provider-generated signed timestamp that enables end users to check when the content was signed. If the content was signed when the cert was valid, then the content is authenticated and considered safe.



1. *Dataquest Insight: Application Stores; The Revenue Opportunity Beyond the Hype*, Gartner, Inc., January 2010
2. *The Anti-Phishing Working Group*, March 17, 2009



BUSINESS GUIDE

Recent Code Signing implementations also typically include a certificate revocation list (CRL), which is a database that keeps a record of all revoked or expired certs.

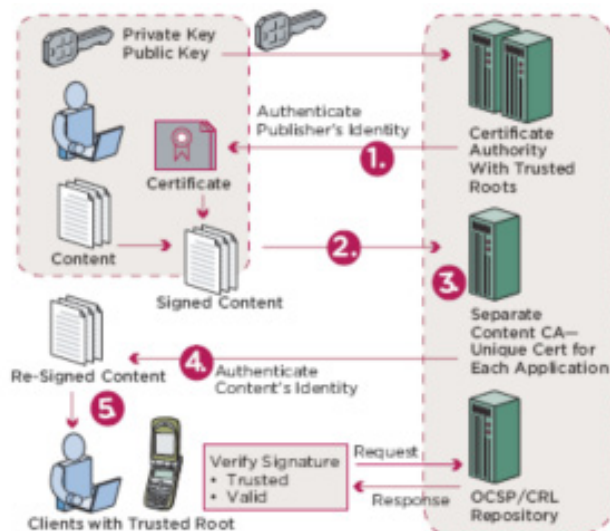
THE SOLUTION

VeriSign® Code Signing Portal offers an ideal solution to meet the diverse needs of mobile application developers, vendors, and consumers. Now offered by Symantec, the Code Signing Portal represents one of the latest innovations in Code Signing technology. The solution leverages more than ten years of experience providing Code Signing services to individual developers, small and large ISVs, and enterprise markets across a variety of platforms, helping them accelerate their applications' time to market and reach more customers.

HOW THE CODE SIGNING PORTAL WORKS

A Code Signing Portal is an advanced Code Signing solution from VeriSign Authentication and Security Business, now a part of Symantec, that authenticates the identity of the publisher as well as the integrity of each piece of signed code. This is how it works:

- **Step 1:** The developer enrolls, and receives a publisher ID certificate that establishes the developer's identity and legitimacy as a software or content publisher.
- **Step 2:** The publisher then uses the Publisher ID to sign a piece of content (or software), and sends it to Symantec. Before production signing, the developer can request test signing with a 12-week Code Signing certificate, if desired.
- **Step 3:** Symantec validates the publisher signature each and every time a piece of content (or software) is sent to Symantec.
- **Step 4:** Once Symantec confirms the signature is from a valid Publisher ID, Symantec strips the publisher's signature, generates a new key pair from a different Certificate Authority (dubbed "Content CA"), signs the content using this private key, destroys the private key associated with the Content ID for added security, and sends back the content to the publisher with the newly generated Content ID. All this happens seamlessly and instantaneously within the Symantec infrastructure.
- **Step 5:** The "re-signed," or authenticated, content is now ready for trusted distribution.



When the end user downloads a VeriSign-signed application, the client device that has the embedded Content CA root checks the validity of the Content ID by sending a request to the CRL/Online Certificate Status Protocol (OCSP) repository maintained by Symantec. If the Content ID is revoked (i.e., it appears on the CRL/OCSP repository), then a warning lets the user know the content should not be trusted. Otherwise, the content signature is verified and the user can download the application/content onto the mobile device. A single signature verification at the client device level is all that is required because Symantec has already verified the publisher's identity.

The Code Signing Portal also features centralized web-based application management and signing services. To sign a new application, developers visit the signing portal, enter the application name, a version identifier, and select the signing service they wish to use. After using the portal to upload the file, developers can request a digital signature for the application simply by clicking the "Sign" button. The portal also provides a full audit trail so developers can track and view every step in the Code Signing process.





BUSINESS GUIDE

SUPPORTED PLATFORMS

VeriSign Code Signing Portal is currently available for the Microsoft® Windows Mobile platform at www.verisign.com. The VeriSign Code Signing Portal also supports private signing services for platform and service providers, as well as enterprises.

BENEFITS

VeriSign Code Signing Portal provides a host of benefits for individual developers, ISVs, and enterprises. For end users, Code Signing verifies publisher identity, providing protection from malware infections, identity theft, and other cybercrime.

For software publishers, Code Signing allows developers to comply with security requirements, protecting their customers while accelerating an application's time to market and expanding its reach. A Code Signing Portal also:

- Provides granular revocation capabilities for software publishers
- Simplifies traceability of buggy or rogue applications
- Provides greater security by making code harder to compromise
- Minimizes risk of expired or revoked publisher status
- Enables publishers to control the lifespan of each application with greater visibility

SUMMARY

Designed to be adaptable, VeriSign Code Signing Portal offers a versatile, easy-to-manage Code Signing solution that allows developers to create applications for specific mobile platform vendors and enterprises. For example, software development houses may use enterprise-class Code Signing to secure internal applications. Software testing companies can use this service as part of their certification process, either internally or as part of a requirement by their customers. Firmware development companies can use customized Code Signing services to help ensure their firmware's integrity. With a Code Signing Portal, Symantec has taken the Code Signing process to the next level of security and reliability for the mobile applications market.

Visit us at www.Verisign.com for more information.

