Boost Software Adoption and Sales with Code Signing

What's code signing?

Code signing is a digital signature added to software and applications that verifies that the included code has not been tampered with after it was signed.

Code signing increases sales and adoption because customers are able to see proof that your product's code has not been infected by hackers.

What are the benefits?

Establish trust. Trust promotes user adoption. When users click to download an application, they see a pop-up dialogue box displaying the publisher's identify that has been verified and confirmed by a trusted certificate authority (CA) like Symantec.

Increase adoption. Code signing eliminates disruptive security alerts that might turn away customers or increase support inquiries. Both unsigned and self-signed code trigger security alerts to show that the software publisher is unknown and could be detrimental to the system. The more warnings a customer sees, the less likely they are to commit to downloading your software.

Protect intellectual property. Code signing makes it extremely difficult for criminals to use your company name to distribute counterfeit software or to tamper with your code.

Build confidence with Extended Validation (EV). EV Code Signing offers a more secure process of signing code, allows for greater confidence in the integrity of your application and provides a more frictionless experience for users downloading your application. EV Code Signing is more secure because of its particularly stringent authentication process. It also requires a hardware token and secure PIN for the signing process, which can only be used by the designated developer.

What happens if you *don't* have code signatures on your downloads?

Lost trust. Users will have no information about the publisher's integrity and may not feel safe continuing with installing or using the software.

Errors. Some software will not run without being protected by code signing. Many third-party software publishers and mobile network providers require code signing in order to protect their users.

How do you obtain a code signature?

To obtain a private code signing key, work with an established CA, like Symantec, that can generate a private key for you. You want to be sure to select a reputable CA that will enable you to distribute your software in the ways you need.

Why choose Symantec?

Symantec provides certificates for a wide range of desktop and mobile platforms, including Windows Phone and Android.

Symantec offers superior encryption that's 64,000 times stronger than industry standard (RSA) certificates, with daily malware scans, vulnerability assessments, warranty protection and installation tools.

To learn more about how to protect your software applications with a code signature from Symantec, contact us today.

For global offices and contact numbers, please visit our website.

For product information in the U.S., call:
1-866-893-6565 or 1-520-477-3111

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

For product information in Asia Pacific, call:
Australia: +61 3 9674 5500
New Zealand: +64 9 9127 201
Singapore: +65 6622 1638
Hong Kong: +852 30 114 683

Symantec Website Security Solutions Pty Ltd
3/437 St Kilda Road, Melbourne, 3004
ABN: 88 088 021 603
www.symantec.com/en/aa/ssl-certificates

For product information in the Americas (Non-U.S.), call:
Mexico: 554 738 0448
Brazil: 800 038 0598

For product information in the U.K., call:
0800 032 2101 or +44 (0) 208 6000 740

Symantec (UK) Limited
350 Brook Drive
Green Park, Reading
Berkshire, RG2 6UH UK
www.symantec.co.uk/ssl

For product information in Europe, call:
+353 1 793 9053 or +41 (0) 26 429 7929
Germany: 0800 128 1000
France: 0800 90 43 51
Spain: 900 93 1298

Follow Us:

Symantec Website Security™