PROTECT YOUR APPLICATIONS—AND REPUTATION—WITH SYMANTEC EV CODE SIGNING

White Paper

# Protect Your Applications—and Reputation—with Symantec EV Code Signing

Symantec

# Protect Your Applications—and Reputation—with Symantec EV Code Signing

## Contents

## Introduction: Extra Vetting for Added Assurance

One out of every 14 programs downloaded today is later confirmed as malware.[1] That actually represents a decline from years past: the overall number of new unique malware attacks grew by 2 to 6 percent between 2010 and 2011, compared to 20 percent in the previous year.[2]

Yet even as malware attacks decline in frequency, they become increasingly sophisticated. These new threats exploit vulnerabilities in traditional Internet security, calling into question many security experts' assumptions about how to keep both government and corporate sites secure from invasive malware.

In light of these emerging threats, how do developers provide users with reassurance that an application is safe to download? Just as important, how can developers with well-established reputations avoid the warning messages increasingly issued by operating systems and browsers when users attempt to download any newly developed application?

For years, developers have known that one of the best ways to reassure users is by *signing code*—along with each and every update to it—using a digital signature accessed via a private key issued by a respected certificate authority. In this way, developers can show that the application comes from a trusted source with an established reputation built on thousands of safe downloads.

Signed code has indeed proven very effective, but it is not invulnerable. Due to lax key security, along with vetting processes that range from stringent to nonexistent, malware has found ways to infiltrate even applications with signed code.

Extended Validation (EV) Code Signing Certificates go a long way toward halting that infiltration by requiring a rigorous vetting process to verify the reputation of certificate holders and helping ensure that private key security cannot be compromised. Unlike standard code signing certificates, EV certificates require a hard token and associated PIN in order to sign code, introducing a more secure physical factor of authentication to the signing process. The EV Code Signing process can also provide browsers, operating systems, and security software an additional source of confidence in applications signed with an EV certificate.

This white paper provides key background on the latest malware threats, explains why EV Code Signing Certificates represent the next step in advanced application security, and concludes with proof of these certificates' effectiveness.

## The Threat: Malware's Next Generation

*"A stealthy attack that spreads through the auto-update mechanism of an operating system or software has long been a nightmare scenario for security researchers. On June 7, an analysis of the targeted attack, known as Flame, found that the espionage program could do just that."*

**—Robert Lemos, eWeek[3]**

1. Microsoft IE Blog, "SmartScreen Application Reputation in IE9," May 2011.
2. Total Defense, "2011 Internet Security Threat Intelligence Report," March 2012.
3. eWeek, "Flame Malware's Forged Certificate Suggests Nation-State Effort," June 11, 2012.

If organizations are to stop malware from infecting their networks, they need to do it at the front door—by not downloading or running the infected code in the first place. The best way to do this is by ensuring that any downloaded application comes from a known and established source.

That's not as easy as it used to be. June 2010 brought the arrival of Stuxnet, the first known malware to spy on and subvert industrial systems, now confirmed as the joint creation of the U.S. and Israeli governments.[4] An even more advanced form of "mega-malware" known as Flame, described by researchers as "a complete attack toolkit designed for general cyber-espionage purposes," emerged in May 2012.[5] These new forms of malware are especially dangerous because they truly appear legitimate, complete with signed code and a certificate from a respected issuing authority.

Meanwhile, as malicious code successfully escapes detection, many new applications fall under unnecessary suspicion simply because they are new—even if the developer is well-known and no clear reason exists for considering the code unsafe. What can organizations do to protect themselves from genuine threats without falling under undue suspicion themselves?

For many, the answer is nothing. According to a 2011 study by M86 Security and Osterman Research, 49 percent of responding companies acknowledged that security breaches had occurred but accepted them as a cost of business. That cost may seem unreasonably high when you consider that 59 percent of the survey respondents who reported a financial loss in the wake of a malware attack estimated their losses to be as much as $50,000.[6]

Clearly, developers must turn to an additional level of assurance in order to build and maintain users' trust. Otherwise these emerging threats will find more ways to exploit the weaknesses of current security measures—and cause lasting damage to users' confidence as a result.

## The Protection: EV Code Signing Certificates

For years, software developers have been using code signing certificates to provide proof of their code's authenticity and legitimacy. While signed code is certainly safer than unsigned code—roughly 98.7 percent of all unique detected threat files in the second half of 2009 were unsigned—sophisticated hackers have begun to find ways around it.[7] They do so by exploiting weaknesses in key security or by taking advantage of the less-than-stringent vetting processes of some certificate authorities.

EV Code Signing closes these gaps to keep malware out. Like Extended Validation (EV) SSL, EV Code Signing was developed by the CA/Browser Forum (CABF) to serve as an industry-wide standard.[8] CABF developed strict guidelines that companies must comply with to earn the EV label for their code signing certificates, along with a lengthy vetting process to verify an organization's identity and trustworthiness.

4. Ars Technica, "Confirmed: US and Israel Created Stuxnet, Lost Control of It," June 1, 2012.
5. PC Magazine, "Massive 'Flame' Malware Stealing Data Across Middle East," May 28, 2012.
6. M86 Security and Osterman Research, "The Global Malware Problem: Complacency Can Be Costly," June 2011.
7. Microsoft Security Intelligence Report, "Protecting Against Malicious and Potentially Unwanted Software."
8. CA/Browser Forum, "The Issuance and Management of Extended Validation Code Signing Certificates," June 2011.

Specifically, the CA checks domain records to ensure that the applicant's email address is associated with a correct domain, plus it does a much more thorough evaluation of the organization itself, including verifying the organization in fact does exist legally, physically, and operationally, and that the organization's identity matches official records.

EV Code Signing also ensures a new level of private key security by making the keys available on hard tokens that users must have a PIN to access. This represents a significant improvement over the browser-based generation of private keys, which could then be filed, emailed, and shared at will, often resulting in lost or stolen keys—and malicious malware attacks like Stuxnet.

With more advanced security, all parties involved — including browsers, operating systems, security software, and end users — can be more confident that the code within a given application or piece of software is safe to download. Browsers, operating systems, and security software can then take EV code signing signatures into account when building or assigning reputation to an application.

## The Proof: Microsoft SmartScreen Filter

For an example of this practice in action, one need to look no further than Microsoft – the first major entity to integrate EV Code Signing Certificate status with its SmartScreen® reputation services (already included in IE9, and built into Windows 8). For developers, this inclusion changes everything, since any application signed with an EV Code Signing Certificate can immediately establish reputation with SmartScreen reputation services, bypassing those unsafe and unknown code warnings that serve as potent deterrents to downloading software. For new companies and developers this is a real boon: otherwise they would need to build reputation over a much longer period of time through a pattern of successful downloads. Users also benefit by knowing and having confidence that the application they are downloading is from a developer that is trusted by a globally recognized CA.

SmartScreen for IE9 goes beyond the URL-based protection provided by IE7 and IE8, adding protection at the application layer. This is called SmartScreen Application Reputation, which addresses the limitations of block-based approaches, since websites are often unable to identify new attacks until applications have been confirmed as malicious. SmartScreen uses reputation as a significant part of its evaluation, helping protect users from newly released malware programs while removing unnecessary warnings for publishers who have an established positive reputation.

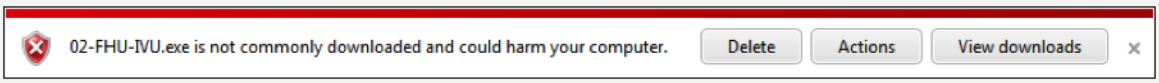
More than 50 percent of programs with no reputation are new to the Web. Of the programs that trigger an Application Reputation warning in IE9, 25 to 70 percent are later confirmed as malware.[9]

9. Microsoft IE Blog, "SmartScreen Application Reputation in IE9," May 2011.

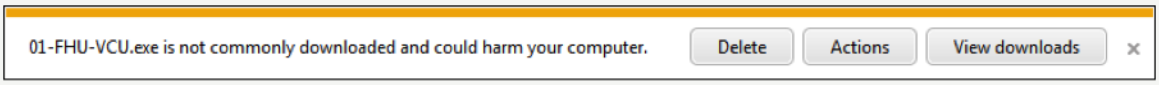
### Application Reputation In Action

Microsoft SmartScreen Application Reputation for IE9 clearly differentiates between known and unknown publishers, and gives special treatment to applications protected with EV Code Signing Certificates.

SmartScreen for IE8 produces a red warning bar for any new application, regardless of publisher.




For applications protected with a traditional code signing certificate, IE9 issues a yellow bar indicating that the app is "signed and unknown," thus helping users understand that the publisher is a trusted entity.




If an application is signed with an EV Code Signing Certificate and contains no malware, IE9 grants that application immediate reputation, and a user's download avoids SmartScreen filter warnings altogether.

Without an EV Code Signing Certificate, developers' work will be blocked by the SmartScreen filter. Even if you sign a piece of code with a regular code signing certificate, SmartScreen might still produce a warning and thus cause a user to hesitate before downloading your code.

For Microsoft, the results of implementing the SmartScreen filter in IE9 have been nothing short of spectacular. Since the release of SmartScreen, IE9 has blocked 1.5 billion malware attacks and 150 million phishing attacks.[10] In addition, Microsoft believes that the Application Reputation provided by EV Code Signing Certificates will prevent more than 20 million additional infections per month (on top of existing SmartScreen URL reputation blocks).[11] And because programs and publishers can now establish reputations, 90 percent of program downloads no longer show browser security warnings when SmartScreen is enabled.[12] In other words, warnings are only displayed when the risk is high—with typical users seeing just two warnings per year.

### Microsoft SmartScreen for IE9: By the Numbers

- **1.5 billion** malware attacks blocked
- **150 million** phishing attacks blocked
- **20 million** infections prevented per month
- **90 percent** of programs downloaded safely with no browser security warnings

### Symantec EV Code Signing Certificates for Microsoft Authenticode

With the public release of the CABF guidelines, SSL providers will begin to offer their own versions of EV Code Signing Certificates. These offerings will all observe the basic standards set down by CABF, but developers should look to Symantec EV Code Signing Certificates for the following reasons:

- **Trusted.** Symantec is the #1 code signing provider to developers and publishers around the globe.
- **No Hidden Costs.** While some CAs may require customers to purchase tokens separately, Symantec EV Code Signing includes a hardware token.

10. Ibid.
11. Ibid.
12. Ibid.

- **Secure.** The Symantec hardware token complies with FIPS 140-2, the gold standard for cryptographic security.[13]
- **Current.** Symantec offers an optional timestamp to show when code was signed, bolstering users' confidence while reducing the cost of code maintenance.

Symantec EV Code Signing Certificates work hand-in-hand with Microsoft Authenticode, a technology that identifies the publisher of signed software and verifies that it hasn't been tampered with, before users download software to their PCs. Microsoft IE and its SmartScreen filter help ensure security by identifying and blocking downloads of malicious Java applets, plug-ins, Microsoft ActiveX controls, and other executables on IE9 and Windows 8. Additionally, the Symantec offering supports Silverlight 4 applications and complies with security requirements for the Microsoft Azure cloud platform.

Together, Symantec and Microsoft can help ensure that users can navigate the next-generation Windows 8 operating system without worrying about the legitimacy of the applications they download. No other code signing provider can offer the same level of industry leadership, commitment to security, and tight integration with Microsoft.

## Conclusion

With malware growing more ambitious and sophisticated each day, organizations must evolve their security efforts to keep up. Traditional code signing certificates are simply no longer sufficient to prevent a new generation of malware attacks.

Enter EV Code Signing Certificates, which rely on a higher level of key security to prevent infiltration from even the most advanced malware attacks. With adoption of the EV Code Signing standard into the Microsoft SmartScreen filter for IE9 and Windows 8, developers have a new tool for blocking unwanted applications without deterring users from downloading legitimate apps.

The value proposition of EV Code Signing Certificates will continue to increase as more and more security software, operating systems, and browsers follow Microsoft's lead in using EV Code Signing Certificates to establish immediate reputation. With these new standards in place, users will have no need to question the legitimacy of known publishers, and will only be alerted to the presence of applications that pose a genuine danger. That way, they can focus more of their attention on enjoying the Internet—not fearing it.

13. National Institute of Standards and Technology Computer Security Division, "Security Requirements for Cryptographic Modules," December 2002.

## More Information

### Visit our website

http://go.symantec.com/code-signing

### To speak with a Product Specialist in the U.S.

Call 1 (866) 893-6565 or 1 (650) 426-5112

### To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

### About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

### Symantec Corporation World Headquarters

350 Ellis Street
Mountain View, CA 94043 USA
1 (866) 893 6565
www.symantec.com