



WHITE PAPER

Maximising Site Visitor Trust Using Extended Validation SSL





CONTENTS

+ The Erosion of SSL's Identity Promise	3
+ Introducing Identity Visitors Can Trust	4
Internet Explorer 7: Green for Go	4
+ How Extended Validation Works	7
+ EV Upgrader Extends Protection to Windows XP Clients	8



Web business faces a crisis in confidence. Trust in site security is declining, and in increasing numbers consumers are scaling back their online transactions—or opting out entirely. According to Forrester Research on December 8, 2005, an astonishing 24 per cent of Internet users reported that they would not be shopping online that holiday season because they did not feel safe. A full 61 per cent reported that they had at least reduced online purchases for the same reason. While this phenomenon has been masked by the overall increase in online activities like banking, trading securities, and filing taxes, the fact remains that many online retail businesses are less effective than they could be and are leaving money on the table.

Starting early in 2007, online companies will be able to definitively demonstrate their identity to customers—and customers will be able to confirm this identity before trusting sites. This opportunity comes as a result of the greatest development in the Web's secure backbone in over 10 years. It is the introduction of a new kind of SSL Certificate, the first since the technology's origin more than a decade ago.

These new certificates are called Extended Validation (EV) SSL Certificates, and they represent more than a year's effort by the CA/Browser Forum, an industry consortium of leading Web browser manufacturers and SSL certification authorities (CAs) such as VeriSign. Starting late in 2006, members of the CA/Browser Forum have made these new certificates available for the benefit of Web businesses and site visitors alike. The certificates can facilitate online commerce in all its forms by increasing visitor confidence in legitimate sites and greatly reducing the effectiveness of phishing attacks.

The Erosion of SSL's Identity Promise

Ask your typical online shopper what the little lock icon on her Internet browser means, and she will tell you it means that transmissions are encrypted and therefore protected from spying eyes. While that is technically correct, it is not all that the original pioneers in e-commerce intended it to signify.

The original purpose of SSL Certificates was to validate the identity of a site when a user connected to it. That is because although it is difficult to mimic physically the identity of a business, it is quite easy to mimic one online. The industry understood this principle as early as 1995 and therefore invented SSL Certificates. The creators intended the certificate to vouch for site identity and therefore protect online shoppers from scams. In the beginning the identity promise of a standard SSL Certificate was enough. Today, however, it is not. The widespread use of the Web by laypeople with no special level of computer education—combined with the low visibility of the lock icon on popular browsers—have made it possible for phishing to become the phenomenon we see today.

Despite original intentions, traditional SSL Certificates are not the solution. While some CAs do a very good job of authenticating identity, others do very little or employ easily fooled practices. A site can even use a self-signed SSL Certificate with no identity authentication whatsoever. In the second half of 2005 online users began to see large scale phishing attacks that used low authentication, “soft-target” SSL Certificates to further the illusion of legitimacy.

Introducing Identity Visitors Can Trust

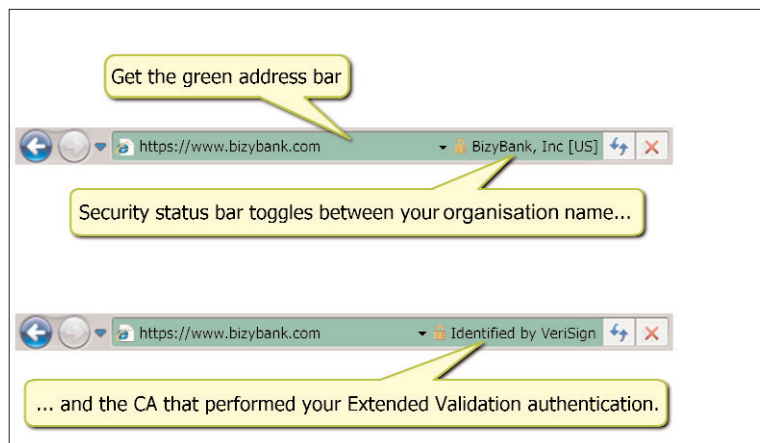
For SSL Certificates to reclaim their authority as a source of site identity information for visitors, industry leaders needed to shore up two weaknesses in the existing system. First, the industry needed a new category of SSL Certificate that carries a high level of promise regarding a site owner’s identity. Then it needed a browser interface that makes it easy for users to see that identity when it is known—and recognise when it is not. These new certificates are the EV SSL Certificates mentioned previously. Some users also refer to them by their working name, which is High Assurance (HA) SSL Certificates. These differ from generic “high assurance certificates”, which do not imply EV status.

The CA/Browser Forum, consisting of over 20 leading Web browser manufacturers, SSL Certificate providers, and WebTrust auditors, worked over a year in co-operation with the American Bar Association Information Security Committee (ABA-ISC) to create a standardised authentication process that every CA must follow to issue EV certificates. Such CAs must undergo independent audits to confirm compliance with the specified process. The CA/Browser Forum built this process on existing business verification practices that have been successful over years of widespread use in authenticating millions of SSL Certificates.

Once a CA completes authentication according to this process, it may issue a certificate with EV status. This certificate operates exactly like a traditional SSL Certificate. In fact, browsers not built to recognise EV certificates (including Windows® Internet Explorer® 6, Mozilla® Firefox® 2.0, and their predecessors) behave exactly as they would with a non EV certificate. New EV-compatible browsers, however, display these certificates in highly visible and more informative ways. The first such browser is Internet Explorer 7 (IE7).

+ Internet Explorer 7: Green for Go

IE7 has added several interface conventions to enhance identification of site ownership. Most obvious is the “green address bar”. When an IE7 browser accesses a page with a valid EV certificate, the background of the address bar turns green. This simple change indicates very visibly that a site has undergone high level identity authentication. The choice of colour also employs demonstrated interface conventions. In the vocabulary of desktop interface design the colour green signifies “safe to proceed”, just as red signifies danger or a warning.





Consumer research indicates that these interface conventions are highly effective. In the autumn of 2006, VeriSign conducted usage and attitude research with online shoppers across the United States. VeriSign's findings included the following:

- 100 per cent of participants noticed whether or not a site showed the green Extended Validation address bar.
- 100 per cent of participants were more likely to share their credit card information with sites that showed the green address bar.
- 98 per cent of participants preferred to shop on sites that showed the green Extended Validation address bar.
- 80 per cent of participants reported that they would hesitate to shop at a site that previously showed the green Extended Validation address bar and that no longer does so.

IE7 also contains an additional field to the right of the address bar, called the Security Status Bar. This field appears when the browser can offer information that may be useful to site visitors in evaluating sites. On pages with EV SSL Certificates, the Security Status Bar displays the organisation name. This text string comes directly from the certificate, where the CA placed it. Because the CA verified this name and the browser displays the name in its own interface, a visitor can rely on the accuracy of this string.

In the example of the hypothetical online bank called BizyBank, the institution's name appears directly in the browser interface. End consumers can verify the site's identity by looking for the green address bar and the name BizyBank, which together present a significant new obstacle to phishers seeking to take over BizyBank accounts. Today a phisher need only duplicate the original site and find a convincing URL to be up and running. If BizyBank's customers learn to seek the company's name and a green address bar before providing confidential information, then a would be phisher will not be able to mimic this interface. Even if the phisher used an existing business to purchase EV certificates for the phishing site, the browser interface would not contain the name BizyBank.

The Security Status Bar also contains the name of the authenticating CA, enabling customers to consider the security employed by sites before choosing to do business. If site visitors do not trust the chosen SSL Certificate provider, they can take their business elsewhere. Likewise, if a CA issues bad EV certificates, the public will learn not to trust sites using this SSL Certificate brand.

Research indicates that the choice of SSL Certificate brand can affect a site visitor's propensity to engage in transactions. For example, leading European travel company Opodo tested a set of identical online order pages with and without the VeriSign Secured Seal™ and found that the pages with the seal received a 10 per cent increase in sales over those without it. Said Warren Jonas, Opodo's head of service management, "We immediately realised the impact that the trust factor can have on shopping basket abandonment rates and we have since published the VeriSign seal on all the payment pages across our network of European sites."

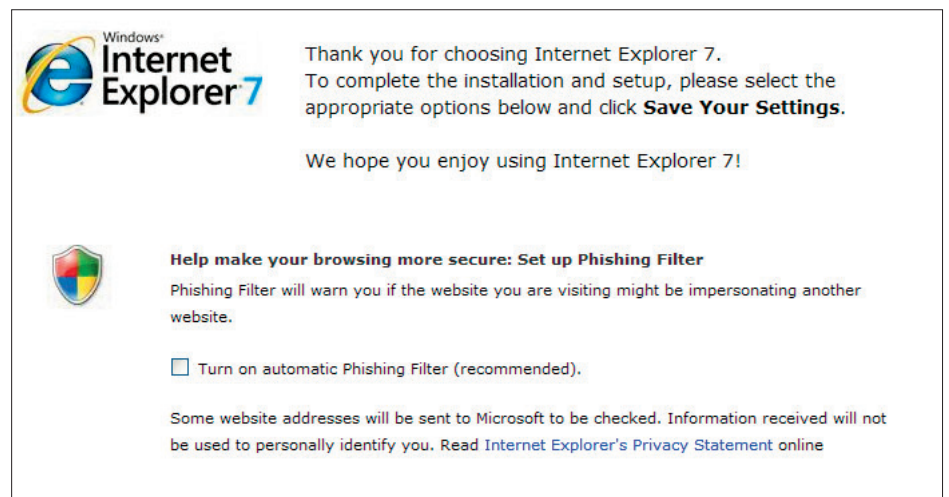
In the summer of 2006, prominent market research firm TNS studied online shoppers' reactions to a variety of online security seals and determined that the VeriSign Secured Seal is far and away the world's most recognised online trust mark. The research indicates that 56 per cent of worldwide online shoppers recognise the VeriSign Secured Seal—a percentage eight times greater than the next most recognised SSL Certificate brand.



These results highlight the importance of the SSL Certificate security brand online retailers choose to display on their sites. Choosing to display the Web's best-known security brand could increase the number of transactions—and therefore a site's overall effectiveness as an online business—by 10 per cent or more.

Certain settings in IE7 can affect the display of these interface conventions. In particular, for the interface to exhibit these behaviours, the browser needs to have its Online Certificate Status Protocol (OCSP) function enabled. OCSP makes it possible for a browser to check SSL Certificates in real time to ensure they have not been revoked. Most recent browser releases support OCSP and at the same time contain a control in the interface that allows it to be turned off. Because of the high trust promise of EV certificates, IE7 requires OCSP to be enabled for it to display green address bars and other EV interface conventions to any EV certificate. That way the user knows not only that this site underwent a high level of identity authentication but also that no incidents have occurred subsequently to require the revocation of this certificate.

In addition to enabling OCSP directly, IE7 can also automatically enable this ability when the user turns on another feature in the product that requires OCSP. This feature is called Phishing Filter, and it augments the EV functionality by providing red or yellow coloured address bars on sites that meet certain trigger conditions categorising them as suspicious sites. IE7 makes it possible to enable this feature right during installation and recommends that the user do so. Enabling Phishing Filter enables the EV interface as well.



Enabling Phishing Filter (as recommended during installation) automatically enables EV SSL as well.

The Windows Vista™ operating system goes even further. In IE7 for Windows Vista, OCSP functionality and the Phishing Filter are defaulted to on, and the browser user has to actively disable them for them not to function.

It is impossible to measure what percentage of client systems with IE7 have OCSP enabled. Considering the high value to end consumers of the EV green address bars and Phishing Filter, these features' visibility in the interface, and Phishing Filter's recommended status during installation, VeriSign estimates this percentage to be quite high. Site administrators evaluating EV SSL Certificates should make sure these capabilities are enabled on their own systems. Green address bars will never display on a copy of IE7 that has these features disabled.

How Extended Validation Works

The EV architecture has been designed to offer reliable Web site identity information to end consumers so that they can make the best possible decisions about which sites to trust. Achieving this mission has required modification to every component of the Web's trust architecture. In addition to the new, highly understandable interface conventions, EV certificates owe their dependability to 1) modifications in authentication procedures and 2) real time certificate checking.

- 1) The first step is authentication. The CA/Browser Forum carefully crafted the EV authentication guidelines over the course of more than a year to ensure that the results of authentication were reliable. These guidelines require qualified CAs to use primary or authenticated information instead of self-reported information from certificate requestors. They employ the proven techniques that have successfully authenticated millions of certificates in over a decade of use. This procedure ensures that all information in the certificate is accurate and that the certificate requestor has the authority to obtain this certificate for this organisation. These authentication procedures are available for public examination at www.cabforum.org. Each CA is required to undergo a yearly audit by a registered WebTrust auditing firm to ensure that it is following the EV guidelines correctly.
- 2) Once a certificate is issued, the next step is to ensure that the certificate presented to the customer accurately reflects what the CA discovered and that certificates purporting to meet the EV authentication standard actually do so. Certificate integrity is assured because every SSL Certificate includes secure hash functions and will not work correctly if tampered with in any way. The EV infrastructure goes on to ensure that the certificate exists in good standing by using real time certificate validity checking. This checking depends on two parallel infrastructures. The first is OCSP, mentioned earlier. OCSP performs a real time revocation check for each certificate so that if an EV certificate is compromised or for some other reason requires revocation, that certificate will not appear as valid on EV compatible browsers.

The second real time service is the Microsoft® Root Store. A very simple metadata marker indicates each EV certificate's status as such. To protect against the contingency that an unprincipled or incompetent CA might incorrectly issue certificates marked as EV certificates even though they have not undergone correct EV authentication, the IE7 browser performs a real time check against the Microsoft Root Store to ensure that this SSL root is approved for EV certificates. Because of this check, if a CA were to issue certificates with the EV marker even though that CA was not approved to issue EV certificates, those certificates would still not activate the green address bar and the other EV interface enhancements. Likewise, if an existing CA were to fail its annual audit or repeatedly issue incorrect certificates under the EV banner, Microsoft would then have the ability to remove that root from the list of approved EV roots in the Microsoft Root Store. This action disables green address bars and other EV interface elements for all certificates issued against this suspect root.



EV Upgrader Extends Protection to Windows XP Clients

While the EV interface elements occur automatically for Windows Vista clients visiting a site, IE7 on Windows XP requires an SSL root update before the browser is able to display EV certificates as such. VeriSign has created VeriSign® EV Upgrader™, the first ever solution to enable all visiting IE7 browsers to detect EV SSL Certificates and display them appropriately. EV Upgrader takes advantage of existing root update capabilities in the Windows operating system to automatically and invisibly download and install the new EV root on the client system. To make EV Upgrader as easy to use for site administrators as possible, VeriSign has built it right into the VeriSign Secured Seal—including the VeriSign Secured Seal you may already have installed on your site.

For a comprehensive description of EV Upgrader and how it works as part of the VeriSign Secured Seal, see VeriSign's white paper, *EV Upgrader: Enabling Windows XP Clients for Extended Validation*. To learn more about VeriSign EV certificates or to purchase them for your site, see <http://www.verisign.co.uk/ssl/index.html>.