

Extended Validation SSL Certificates

A NEW STANDARD TO INSPIRE TRUST, *improve
confidence and increase sales ...*

INDEX

- 1. Extended Validation (EV) SSL Certificates – solving a trust problem*
- 2. Traditional SSL – not the assurance it used to be*
- 3. EV SSL Standard – more trustworthy, more visible*
- 4. Green – immediately identifiable interface improvement*
- 5. IE7 Settings – real-time validity checks*
- 6. EV – authenticity, integrity, validity*
- 7. EV UpgraderTM – Windows XP client benefits*
- 8. SSL Web Server Certificate with EV – a trusted thawte solution*

1. Extended Validation SSL Certificates – solving a trust problem

Many consumers don't trust web site safety enough to complete an e-commerce transaction. The frequency of malicious web schemes such as phishing and pharming creates an environment of fear and reticence. Gartner recently reported that in 2006 41.2% of online adults in the U.S definitely received Phishing emails, 46% changed their purchasing and online behavior as a direct result of security concerns and 10% reduced their online spending by at least 50%. As a result nearly \$2 Billion in e-commerce sales were lost due to user concern over security.* Online commerce may still be growing but there are a significant number of people opting out or reducing their spending due to security concerns. If you are a web business that depends on consumers trusting you enough to share their financial, personal or other sensitive data this is an alarming trend. Identity authentication now takes center stage in the fight to shore up consumer confidence in e-commerce.

To combat this problem, leading web browser developers and SSL Certification Authorities (CAs), including *thawte*, joined forces to create a new standard for web site identity authentication. After more than a year of effort, the CA/Browser Forum introduced the new Extended Validation (EV) SSL Certificate. This new standard is the most significant advancement for the World Wide Web's secure backbone since SSL Certificates were first introduced over a decade ago.

Extended Validation SSL Certificates offer web sites a better method for assuring their visitors of their legitimate identity. Browser support for the enhanced features of Extended Validation SSL Certificates began with Microsoft® Windows Internet Explorer 7 in early 2007 and other browsers, such as Firefox and Opera, have announced their intentions to follow in short order.

2. Traditional SSL – not the assurance it used to be

SSL Certificates were created to validate the genuineness of a web site because it is so easy to counterfeit a business on the web. In 1995, when they were invented, a standard SSL Certificate provided adequate protection for consumers. Times have changed; web scams became more sophisticated and these traditional certificates may no longer be adequate. A member of the general public can easily forget to look for the small lock icon in the browser window and they won't necessarily recognize a fraudulent use of an SSL Certificate. Sophisticated web scammers easily fool some less stringent CA identity authentication practices and some web fraud sites simply use self-signed SSL Certificates that provide no identity authentication at all. The general public often cannot recognize when they are presented with one of these questionable certificates. This is one reason why spoofing schemes such as phishing and pharming have become so prevalent and successful.

3. EV SSL Standard – more trustworthy, more visible

The Extended Validation SSL standard helps solve both the problem of low SSL protection visibility and low assurance of a site's genuine identity. The CA/Browser Forum, comprised of over twenty browser manufacturers, CAs, and WebTrust auditors along with the American Bar Association Information Security Committee (ABA-ISC), worked for more than a year to create the first inception of the EV authentication process. The CA/Browser Forum continues to develop the EV standard and guidelines in order to improve Internet security and combat online fraud. The EV guidelines describe a set of standardized best practices that must be followed in order for an SSL Certificate to meet the requirements for Extended Validation status. Any CA who wants to issue EV SSL Certificates must first pass an independent WebTrust audit confirming their use of the EV identity authentication standard practices. The rigorous EV authentication process described in these guidelines relies on business verification practices proven to be effective for authenticating millions of SSL Certificates.

An EV SSL Certificate functions the same as a traditional SSL Certificate for older browsers that do not recognize EV, such as Internet Explorer 6, Firefox 2.0, and earlier versions of both. For new high-security browsers, such as Internet Explorer 7 (IE7), EV offers significantly more benefits than a traditional SSL Certificate. To the end user, these newer browsers display an EV SSL authenticated session in a far more visible and informative way than the small lock icon at the bottom of the page shown for many traditional SSL sessions.

4. Green – immediately identifiable interface improvement

EV contains a number of user interface enhancements aimed at making the identification of an authenticated site immediately noticeable to the end user. IE7 is the first browser to deliver these benefits: by default with Windows Vista and with an easily prompted update for Windows XP.

The most obvious interface enhancement is the green address bar effect; when an EV-enabled client visits an EV authenticated site the address bar turns a highly visible green color. This conspicuous color change immediately notifies the end user that this web site passed a rigorous authentication process. Green is also a highly effectual color – to most people green means go, it is safe to move forward.

Cont... Green – immediately identifiable interface improvement



In addition to the green address bar effect, a security status bar appears to the right of the address bar. This field, also green, displays the name of the organisation responsible for the web site and toggles to identify the CA that authenticated the web site. In the example above, the name of Woodgrove Bank displays in the security status bar field and automatically toggles to the name of the CA (in this case *thawte*). The EV SSL Certificate provides the source for the names in these fields, confirming that the CA has verified this information. Therefore the end user can depend on it being accurate. This interface convention makes it easier for customers to notice the name of the CA. This new higher visibility to customers should motivate web sites to obtain their certificates from only the most reputable CAs. If a customer is not familiar with the CA, they most likely won't trust the web site being certified.

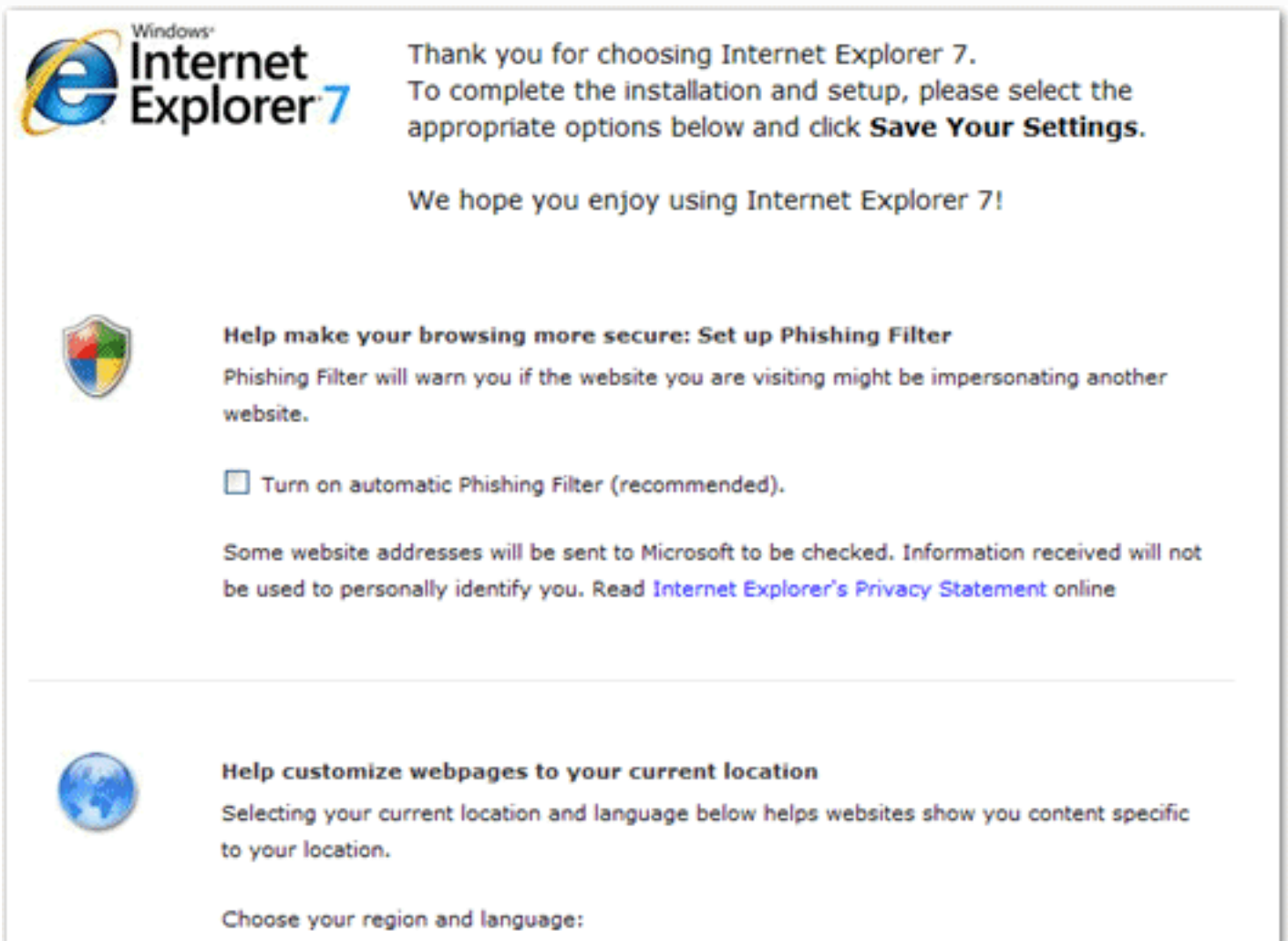
These interface enhancements, difficult to counterfeit by phishers and pharmers, create a new level of protection for web site visitors. If a spoof site buys a traditional SSL Certificate it would not display the highly trusted green address bar and even if they bought an EV SSL Certificate to gain the green address bar, it still would not be able to display the name of the organisation they were attempting to spoof in the security status bar.


5. IE7 Settings -- real time validity checks

Either the Online Certificate Status Protocol (OCSP) function or Phishing Filter within IE7 must be enabled for a client to see the powerful EV interface enhancements.


The OCSP allows a browser to perform a real-time validity verification of an SSL Certificate. This real time check, part of the high level identity authentication aspect of EV, makes sure this certificate has not been revoked. Newer browsers typically support OCSP but this feature may be manually disabled.

The Phishing Filter in IE7 adds functionality in addition to enabling the EV green address bar and security status bar interface. With the Phishing Filter enabled, an end user's address bar turns yellow or red when the user visits sites that IE7 identifies as suspicious. IE7 recommends the user activate the Phishing Filter during installation and the Phishing Filter automatically enables OCSP.




 Thank you for choosing Internet Explorer 7.
To complete the installation and setup, please select the appropriate options below and click **Save Your Settings**.

We hope you enjoy using Internet Explorer 7!

 **Help make your browsing more secure: Set up Phishing Filter**
Phishing Filter will warn you if the website you are visiting might be impersonating another website.

Turn on automatic Phishing Filter (recommended).

Some website addresses will be sent to Microsoft to be checked. Information received will not be used to personally identify you. Read [Internet Explorer's Privacy Statement](#) online

 **Help customize webpages to your current location**
Selecting your current location and language below helps websites show you content specific to your location.

Choose your region and language:

IE7 installation page with the Phishing Filter option. Microsoft recommends users enable the Phishing Filter which allows for the enhanced EV interface to display the green address bar and security status bar.

Windows Vista systems automatically enable both the OCSP and Phishing Filter functions; for these features to be turned off, the end user must manually disable them.

6. EV – authenticity, integrity, validity

Building a system to help end users make better decisions about who to trust on the web required the CA/Browser forum to modify almost every component of the trust infrastructure for the web. The EV standard encompasses far more than just a new user interface, although the new user interface will symbolize to end users the significance of the rest of the work performed. EV SSL Certificates base their strength on specific identity authentication process requirements and real-time certificate validity verification.

authenticity

The CA/Browser Forum spent more than a year developing identity authentication guidelines for EV that would be reasonable to follow and would help produce reliable results. To read the first implementation of these official EV authentication guidelines, visit the CA/Browser Forum web site at www.cabforum.org. EV guidelines require all identity information from certificate requestors be supplied by authenticated third parties or come directly from primary sources. The requesting organisation cannot verify its own identity. This requirement makes sure the identity information being authenticated is correct. The authority of the person requesting the EV Certificate is also verified. Additionally, all CAs issuing EV SSL Certificates must pass an annual WebTrust audit confirming that they are diligently following all the EV authentication guidelines.

thawte requires a signed acknowledgement of agreement from the organisational contact listed on an order for an EV SSL Certificate. A company registration document is also required if *thawte* is unable to confirm the organisation details through a government database. A legal opinion letter may also be requested to confirm the following details about the requesting organisation if *thawte* is unable to verify this information elsewhere:

1. physical address of place of operation,
2. telephone number,
3. confirmation of exclusive right to use the domain,
4. additional confirmation of the organisations existence (if less than 3 years old), and
5. organisational contact's employment status and authorization to purchase EV SSL on behalf of the organisation.

integrity

Security measures in every EV Certificate helps ensure the integrity of the certificate. A secure hash embedded in every certificate helps protect against hacking. If the content of an EV Certificate is altered, this hash assures that the certificate will be disabled.

validity

The validity of every EV Certificate is checked in real-time through both the OCSP infrastructure and the Microsoft Root Store. The OCSP makes a real-time inquiry to see if a certificate has been revoked for any reason. In addition to the OCSP inquiry, IE7 browsers check with the Microsoft Root Store in real-time to verify that the EV Certificate matches an SSL root approved for EV. This check verifies that the CA issuing the certificate is authorized to issue EV Certificates and has not had their status revoked or suspended for any reason.

7. EV Upgrader[™] — Windows XP client benefits

IE7 clients on Windows Vista systems automatically display the EV green address bar and security status bar interface features. However, IE7 clients on Windows XP may need prompting to update their local root store before they get the new EV interface benefits. *thawte* solves this problem by providing all EV SSL customers with EV Upgrader[™], a method for prompting the automatic update for IE7 on Windows XP clients. This update triggers a normal Windows XP function and should be invisible to the end user. After these clients have visited a site with EV Upgrader from *thawte*, they will display the EV interface conventions whenever they visit a web site protected with an EV SSL Certificate from *thawte*. In most cases the new features appear the next time the client refreshes the currently viewed web page or clicks the next EV SSL protected page.

Installing EV Upgrader is very easy. *thawte* embeds EV Upgrader in the *thawte* Trusted Site[®] Seal. Simply put a site seal on your web page and every IE7 with Windows XP client that visits that page will be updated to show the green address bar effect and security status bar whenever they visit a web site protected by an EV SSL Certificate from *thawte*.

To learn more about EV Upgrader, visit the EV Upgrader Overview page at http://www.thawte.com/ssl-digital-certificates/extended-validation/ev_upgrader.html. Or get the EV Upgrader Product Guide from http://www.thawte.com/ssl-digital-certificates/free-guides-whitepapers/pdf/ev_upgrader.pdf.

8. SSL Web Server Certificate with EV – a trusted *thawte* solution

thawte's SSL Web Server Certificate with EV provides the highest level of identity authentication for web sites available today. This EV Certificate also provides 256-, 128-, 56- or 40-bit encryption. The level of encryption enabled for each session depends on the client browser capability and the cipher suite installed on the web server. For more information on *thawte's* SSL Web Server Certificates with EV, visit <http://www.thawte.com/ssl-digital-certificates/extended-validation-ssl-ev/index.html>.