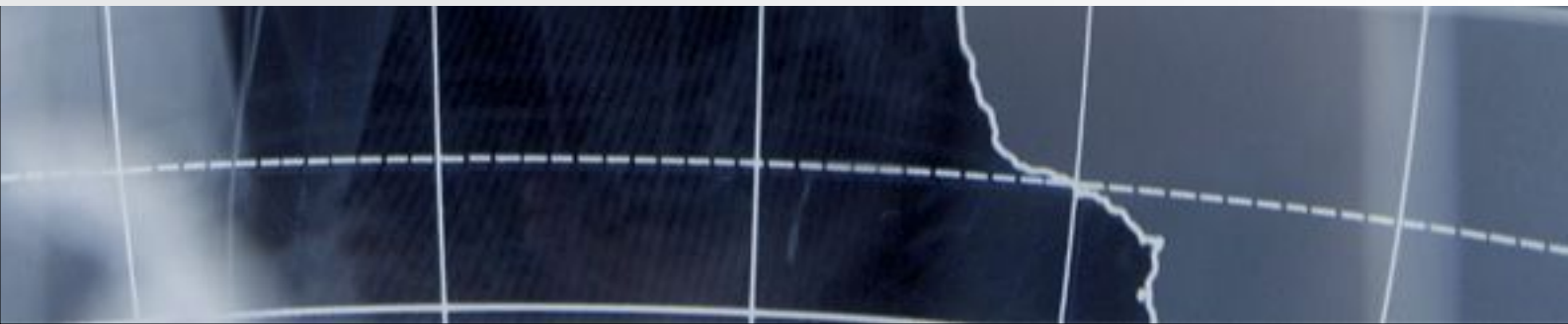
Gain a New Level of Trust with Extended Validation SSL Certificates



Higher Standard for SSL Certificates

Malicious Internet activities such as phishing and pharming have victimized millions of people. The fear these activities generate makes many web users reluctant to complete online transactions with even well-known, reputable companies. To combat this problem the CA/Browser Forum, a roundtable of industry experts, created the Extended Validation SSL standard. Extended Validation SSL aims to improve trust in the online community by standardizing processes for authenticating web sites and making it clear to users when they are on a highly trusted, authenticated site.

The CA/Browser Forum is made up of leading CAs and Internet browser software providers such as Microsoft, the Mozilla Foundation, Opera Software ASA, and KDE. This organization worked to create a higher standard for identity assurance with an authorized set of guidelines for authenticating the identity of a web site. The vetting process for organizations receiving an Extended Validation SSL Certificate is both standardized and more rigorous than SSL Certificates previously offered in the industry.

New versions of major, high-security browsers are expected to present a highly visible green address bar when web users visit web sites with Extended Validation SSL Certificates. In addition to the green address bar, a scrolling field displaying the name of the organization on the certificate and the CA who issued the certificate will appear. This new interface will enable the web site visitor to immediately see that they have opened a secured and authenticated web site and that it is the web site they meant to visit. The first browser to support this new feature is Microsoft® Internet Explorer 7 (IE7).

More Visibility

Browsers typically display a small lock icon at the bottom of the screen to identify that data is being encrypted and that the organization using that web domain has the right to use that domain (as listed in the SSL Certificate securing that web site). With Extended Validation SSL the browser interface display that verifies a secured and authenticated web site is about to become much more noticeable to visitors. New browsers, such as Microsoft® Internet Explorer 7, are expected to distinguish web sites secured by Extended Validation SSL Certificates by turning the address bar at the top of the screen to a highly visible green color. To the right of the green address bar a security status bar will scroll between the name of the organization using that web domain and the CA who issued the SSL Certificate. New browsers will identify a special extension in the SSL Certificate to confirm that it is an Extended Validation SSL Certificate. Older browsers will continue to display all certificates with the traditional lock icon at the bottom of the browser window.

Not just any company is authorized to issue an Extended Validation SSL Certificate. Only CAs who meet certain requirements and pass a WebTrust audit may issue Extended Validation SSL Certificates. New browsers will check to confirm that the CA is authorized before displaying the Extended Validation SSL Certificate. It is more important than ever to select a CA that has an outstanding track record issuing SSL Certificates because browser vendors can remove CA roots from the root store if the CA fails to meet specified requirements.

You can see the new interface style for an Extended Validation SSL Certificate in IE7 in the example below:

Who Should Use Extended Validation SSL Certificates?

Strong identity authentication can help web site visitors feel more comfortable about completing online transactions – especially for financial services and banking, auctions, large online retailers and any site that carries out high-value transactions over the Internet. Any site that is a prime target for online fraud may benefit from having an Extended Validation SSL Certificate. If an organization wants to assure its web site visitors that they are sharing information with the genuine site for that organization, *thawte's* SSL Web Server Certificates with EV are a proven and very visible solution. An Extended Validation SSL Certificate may boost consumer confidence in the web site and may give that web site a competitive advantage over web sites without the same strong authentication assurance. Over time customers, especially anyone sensitive to the risk of phishing or pharming activities, will look for the green address bar before being willing to complete an online transaction.

Although many sites may opt for the high level of assurance offered through Extended Validation SSL, traditional SSL Certificates will offer enough assurance for other purposes. Securing traffic between internal servers is one instance where a traditional SSL Certificate is adequate. Web sites without ecommerce transactions or sites with very light volume are also candidates for traditional SSL Certificates.

Vetting a Web Site

Until the Extended Validation SSL standard was created, the industry had no standard process for authenticating the organization running a web site. The breadth and depth of background checking differs significantly between CAs. Methods for collecting and confirming information vary. They may include either manual or automated information collection based on phone calls, databases, emails and faxes. It is unrealistic to assume that web site visitors know what vetting practices are used by each CA and therefore unrealistic to assume that those visitors understand the strength or weakness of a particular certificate.

With Extended Validation SSL Certificates, the CA/Browser Forum has defined a high assurance vetting process standard. Before issuing their first Extended Validation SSL certificate, a CA must adopt the Extended Validation SSL vetting standard and pass an audit with Web Trust. The Extended Validation SSL vetting process includes verifying an organization's identity and right to use the domain, that the individual purchasing the certificate is legally authorized to request an SSL Certificate for that organization, and that the organization has authorized the request for a certificate. For more information visit the CA/Browser Forum web site at URL; http://www.cabforum.org.

Standardizing the vetting procedure results in SSL Certificates that can be expected to meet the same level of authentication assurance irrespective of who authorized the certificate. The green address bar interface displayed by new browsers clearly identifies sites that have been vetted at this new higher standard. So visitors to a web site with an Extended Validation SSL Certificate will immediately be able to identify and trust that site to meet a high assurance standard without having to read and understand that particular CA's vetting process.

Vetting a Web Site

thawte requires a signed acknowledgement of agreement from the Corporate Contact listed on an order for an Extended Validation SSL Certificate, as well as a legal opinion letter stating that the person requesting the certificate has official authority to obtain and approve an Extended Validation SSL Certificate on behalf of their organization. *thawte* will verify the following information about the requesting organization:

1. physical address of place of operation;

2. telephone number;

3. confirmation of exclusive right to use the domain; and

4. confirmation of an active Demand Deposit Account.

A legal opinion letter is one way for an organization to verify this information for *thawte*. There are alternative methods for authentication and verification if needed. For more information contact a *thawte* customer service representative through the following URL;
http://www.thawte.com/contact.html.

Who Will See the New Interface

Extended Validation SSL is based on the existing SSL protocol and is fully compatible with both newer and older browsers and servers. Microsoft Internet Explorer 7 will be the first browser to adopt the new green address bar interface standard. Users running IE7 on Microsoft Vista operating system will automatically see the green address bar as soon as it goes live in early 2007. Users running Microsoft IE7 on Windows XP, who have enabled the anti-phishing filter, will see the green address bar once they have visited a web site with EV Upgradertm (alternatively they would need to download a patch from the Microsoft Web site). After visiting a site with EV Upgrader, the user will automatically see the Extended Validation SSL green address bar the next time they initiate an SSL session at a site secured by a *thawte* Extended Validation SSL Certificate. *thawte* offers EV Upgrader (a US $300.00 value) to customers as part of their Extended Validation SSL Certificate purchase. Other browser providers, such as Opera, are expected to incorporate Extended Validation functionality in future releases. Older browsers will display Extended Validation certificates in the same manner as traditional SSL Certificates.