

Raising the Bar: Extended Validation SSL Certificates

The Next Generation of SSL Certificates

The explosion of Internet fraud has created intense interest in finding new ways to enhance trust online, reduce online fraud and improve consumer confidence in Web-based transactions. Security vendors and Internet browsers have combined forces to establish the Extended Validation Standard for SSL Certificates (also known as "High Assurance").

The new Extended Validation certificates entail a higher level of business verification than any other certificate on the market, using a thoroughly defined industry-standard vetting process. Major browsers, such as Microsoft Internet Explorer, Mozilla and Opera, intend to give Extended Validation SSL certificates stronger visibility in the user interfaces of their next-generation browsers. With the certificate identity information clearly displayed in new-generation browsers, consumers can discern that they are indeed at the site they think they are, and not a fraudulent version. By creating a new and higher standard for verifying organizations, the Extended Validation SSL certificate standard will help restore the type of business innovation that the Internet promises.

Elevating SSL Information

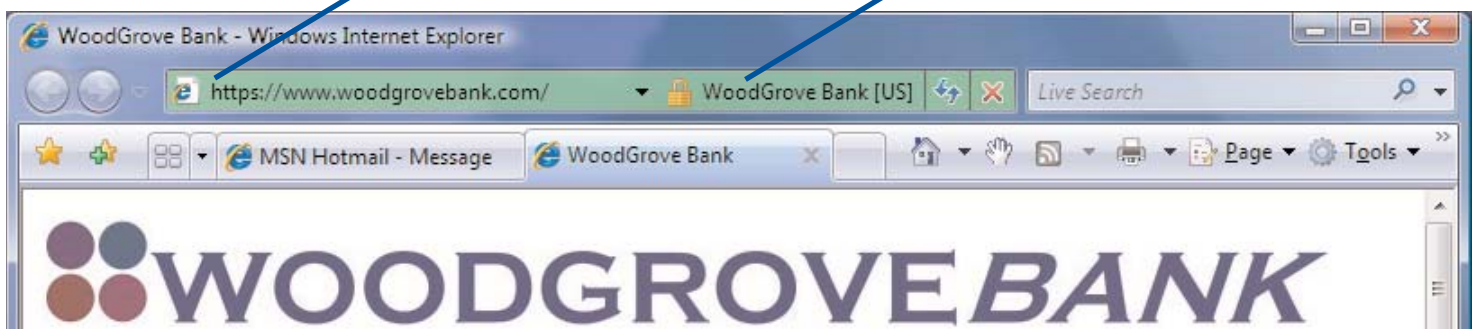
Today, the lock icon fundamentally means that traffic between a user and a website is encrypted and that a CA has identified the Web site and issued an SSL certificate to the person or organization who owns or has the right to use that domain. Next generation browsers and Extended Validation SSL raise the information about SSL certificates typically found in the lower right hand corner of a browser to the top of the browser -- displaying the organizational identity and the issuing CA right in the top address line. The display next to the address bar will toggle between the organization name listed in the certificate and the CA that issued the certificate (GeoTrust, for example). Extended Validation SSL certificates will be identified by the browsers using two criteria - a special extension in the certificate and the validation that the issuing CA is authorized to issue these types of certificates.

Additionally, these next generation browsers will turn the address bar green to signal that a site has been secured by an Extended Validation SSL certificate. Older versions of the browser will display Extended Validation SSL certificates with the same security symbols as existing SSL certificates (i.e. the lock icon in the lower right of the browser window).

Below is an example of a Microsoft® Internet Explorer 7.0 (IE7) browser that displays High Assurance/Extended Validation SSL certificates:

Green URL shows up for
Extended Validation certificates

Security status bar toggles between organization name and the CA
that performed the Extended Validation authentication



Extended Validation SSL Certificates vs. Standard SSL Certificates

Extended Validation SSL certificates are ideal for any organization that has a high-traffic web site, has a high-visibility brand name it would like to protect or a Web site that is likely to be the target of online fraud. The new certificates will not only become an effective anti-phishing tool, but also bolster customer confidence and a businesses competitive edge. If a web site displays these trust marks and a competitor's site does not, the Extended Validation SSL secured site appears to be more trusted and legitimate, a competitive advantage in the ecommerce world. For businesses with a high profile brand, using Extended Validation SSL is a good defense against phishing scams. Customers will learn to look for the green bar before they enter sensitive information online.

Businesses that should use Extended Validation SSL include financial services and banking sites, credit unions, auction sites, large online retailers, and other sites that conduct high-stakes, high-value transactions over the Internet. However, standard SSL certificates will be perfectly valid in many instances -- for example when used to secure traffic between internal servers, to verify the identity of a non-ecommerce web site, to secure ecommerce sites where volume is light or when used on sites that would be unlikely phishing targets.

The Verification Process

Today, there is no industry standard to verify what level of background check was performed on a Web site before being issued an SSL certificate. Verification processes (also referred to as vetting) vary from CA to CA, and encompass an array of manual and automated processes that primarily rely on email or faxed information, database lookups and phone calls. Unfortunately, site visitors have been expected to understand the intricate and highly technical specifications of individual CAs and their Certificate Practice Statements (CPS) in order to comprehend what a given CA does to verify the organizational information contained within the certificate.

The Extended Validation Standard defines the process for certificate validation and the method of display. To enable the heightened security features in new browsers, a CA must adopt the high-assurance certificate validation standard and pass an audit. The validation process requires the CA to authenticate the requestor's domain ownership, organizational identity, employment and authority prior to issuance of the certificate. This uniform process allows consumers and other relying parties to trust an Extended Validation SSL certificate from any participating CA to the same degree, without having to read and analyze every CA's policies and procedures for vetting.

The verification process for Extended Validation SSL certificates will include four key pieces of information:

- Verifying the organization's identity;
- Verifying the organization's ownership or right to use the domain;
- Verifying that the would-be purchaser has the legal authority to make the SSL certificate request for that organizational entity; and
- Verifying that the organization named in the certificate has authorized the request.

Clearing Up the Confusion

Since Extended Validation SSL certificates are built upon the existing SSL protocol, they will be fully backward compatible with browsers and servers available prior to the Extended Validation standard being defined. The new certificates are expected to be available by the end of 2006 or early 2007. Microsoft® Internet Explorer 7 is the first browser to use the new standard in its security status bar, however, it will not be fully functional until IE7 on Vista is launched (expected in 2007).



117 Kendrick Street, Suite 350
Needham, MA 02494
Phone: (781) 292-4100
Toll Free: (800) 944-0492
Fax: (781) 444-3961
E-mail: info@geotrust.com
www.geotrust.com