



White Paper

Extended Validation SSL and Customer Confidence

Suspicion, doubt, reluctance, abandonment, and in some cases refusal to shop online at all anymore are growing characteristics among web consumers today. Despite the overall increase of online activities such as banking and shopping, a disturbing trend has developed. The online business environment is losing the consumer confidence vote and customers, concerned about their security, are spending their money elsewhere.

The Internet brought about changes in the way we do business that made things easier for a lot of people— including criminals. In the brick-and-mortar world, a person would need to acquire the real estate, the staff, and the overall infrastructure to impersonate a physical branch of, say, a popular bank – not a very practical proposition. On the other hand, the Internet allows criminals to mimic the very same bank quite easily. With minimal effort, they can take advantage of the trust customers apply toward mainstream consumer brands. Criminals set up phony “Phishing” sites that look legitimate, yet have nothing to do with the real company they are impersonating. These Phishing sites then harvest sensitive personal data such as passwords, identity numbers and credit card numbers. Phishing and identity theft attacks the very foundation of online consumer confidence and these criminal activities show rampant growth. Gartner reported that in 2006, 41% of adults online received Phishing emails.¹

Any doubt about a site’s legitimacy or security drives customers away – and their money with them. Gartner also reported that in 2006 46% of Internet users changed their online behavior as a direct result of security concerns and that these same concerns cost online businesses nearly \$2 billion. The online community faces a significant business challenge to woo these users back and to prevent current and future consumers from leaving.

These trends spurred the online security industry into action. Recently, an alliance of Certification Authorities (CAs) and browser manufacturers came together to help create a solution to this growing problem. That solution, the most significant improvement to web security in more than a decade, launched early in 2007 in the form of the new Extended Validation (EV) SSL standard.

EV SSL focuses on web site identity validation – key to the fight against the Phishing epidemic. To get a site secured with an EV SSL Certificate, the site owner must pass a stringent, standardized set of identity validation procedures. Once authenticated, the pay-off comes when their EV SSL Certificate displays their higher level of identity assurance more clearly to potential customers. New browsers, such as Microsoft Internet Explorer 7 and upcoming releases of Firefox and Opera, include a greatly enhanced user interface display for web site security – triggered positively by the presence of an EV SSL Certificate or negatively by suspicious activity.

¹ Gartner Research 2006

THE TRADITIONAL SSL SOLUTION: WHAT HAPPENED?

SSL Certificates gained popularity in 1995 to help protect people doing business on the web from online criminals seeking to make money by stealing personal data (especially financial data).

Many people identify SSL with encryption protection, but encryption is only part of what SSL Certificates were intended to do. These certificates are also intended to validate a web site's identity to site visitors. When a visitor visits a web page secured with SSL, the browser interface displays an identifier signifying that an SSL secured session has been initiated to encrypt all data transmitted through the web page and that the site's identity has been verified. The SSL session identifier in the browser window is traditionally a tiny padlock icon at the bottom of the screen and an "s" added to http in the address.

Traditional SSL is still adequate in some instances but there are chinks in its armor. Weak identity vetting and the obscurity of the interface identifiers for the end user undermine the effectiveness of some SSL Certificates.

Identity validation for traditional SSL Certificates lacks standardized procedures. Even today, the process used for identity assurance is strong for some certificates and weak for others. This results in the availability of both high authentication certificates and low authentication certificates and everything in between. Online criminals have figured out that they can work the system to obtain low authentication SSL Certificates for their fraudulent site(s) to help them appear more legitimate.

The lock icon most closely associated with secure SSL web transactions is not prominently featured in a web browser (if it appears at all). The "s" added to the http: moniker is easily overlooked and the SSL Certificate data is buried within an obscure browser menu item. Plus, regardless of whether a certificate has been vetted with high authentication or low authentication procedures, the same user interface conventions are displayed — leading some end users to assume that one SSL Certificate is as secure as any other SSL Certificate.

The confusion created by low authentication certificates combined with low-impact and undifferentiated user interface conventions makes it too easy for malicious web schemes to be perpetrated. A new solution is needed.

EXTENDED VALIDATION: A NEW KIND OF SSL

Representatives from over 25 CAs and browser manufacturers joined together as the Certification Authority (CA)/Browser Forum and along with a number of WebTrust auditors they created the new EV SSL standard. To achieve their ambitious goals almost every aspect of the web's trust structure was adapted to support the new standard.

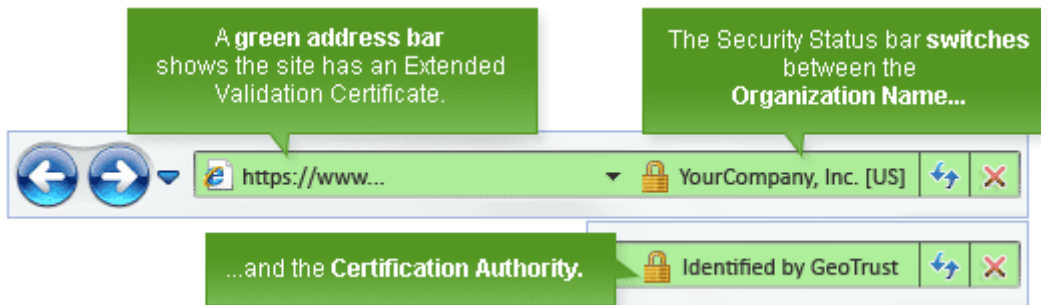
Validity is central to EV SSL – validity of a web site's identity, validity of the issuing CA, validity of the SSL Certificate, and finally clear identification of that validity to the end user. These validity elements result in stricter web site identity vetting standards, real-time certificate revocation checking, stricter WebTrust audit authorization for CAs and highly visible browser user interface enhancements.

At the end of 2006, the new Extended Validation (EV) SSL Certificate standard made its debut. The CA/Browser Forum published the first version of its identity verification process guidelines and the first CAs completed the new WebTrust audits thereafter. In early 2007, Microsoft with IE7 enabled the new browser user interface conventions and revocation checking features (as explained below). Firefox and Opera have already announced plans to do the same for upcoming releases of their browser software.

EV SSL provides the highest level of identity assurance available today from an SSL Certificate. A web site secured with an EV SSL Certificate should instill extra confidence in consumers and help increase the percentage of completed transactions experienced by that web site.

A NEW USER INTERFACE IDENTIFIES A VALID SITE

New high-security browsers, such as IE7 and upcoming releases of Firefox and Opera, display a dramatically enhanced user interface when an end user visits a site secured by an EV SSL certificate. When an IE7 browser encounters an EV SSL Certificate that is authentic and valid, the background in the browser's address bar turns bright green, immediately indicating to the user that the site's identity has been strictly validated by a third party CA. This change of the address bar color is a far more noticeable indicator of site security to an end user than simply displaying a tiny padlock somewhere on the screen. Plus, green is a powerful positive indicator color; green means "it is safe to go ahead" to many people.



The green address bar and security status bar interface conventions clearly identify web sites secured with EV SSL Certificates as legitimate to end users.

The security status bar sits to the right of the address bar. It displays the web site organization's name as it is registered on the EV SSL Certificate. This field provides a secondary, tamper-proof confirmation for site visitors that the site they are visiting is indeed the site they intended to visit. The security status bar also toggles to display the name of the authenticating CA, enabling users to avoid sites using a disreputable CA. Legacy browsers, which were developed before the EV standard, display EV SSL Certificates in the same manner as traditional SSL Certificates.

VALIDITY OF THE CERTIFICATE

EV SSL Certificates are in effect the crème de la crème of the SSL Certificate world and it is important to the industry that these certificates represent a highly-reliable meter for trusting the validity of a web site. This system for verifying the current validity of individual SSL Certificates is always activated in the case of EV Certificates. CAs maintain a revocation record that is checked in real-time every time an end user visits an EV-secured web site. If a particular certificate is found to have been revoked, the address bar will not turn green. It turns red and an error message appears warning the end user that he has accessed a site with a revoked certificate.

There are two methods for checking the revocation lists maintained by most CAs, such as GeoTrust. Traditionally, a browser client would download the entire Certificate Revocation List (CRL) from the CA every time the client visited a web page secured with a certificate. However, this method became cumbersome as these lists grew in size. The newer and more efficient method for checking if an individual certificate has been revoked is via the Online Certificate Status Protocol (OCSP), which does not require the individual download of an entire CRL every time a client visits an SSL Certificate-secured web page. With OCSP, the browser client merely queries the CA data repository regarding the status of a single certificate and the CA server responds either yes, this certificate is revoked or no, it has not been revoked. OCSP is certainly a more efficient and faster method of revocation checking.

IE7 and other recent browsers support the OCSP feature. This functionality can be activated directly or it can be activated when the Phishing Filter is enabled. The Phishing Filter is a valuable feature. In addition to displaying green for an EV SSL Certificate, it will display red (danger) or yellow (caution) in the address bar if the user visits a suspicious site. Both OCSP and the Phishing Filter are automatically activated by default in IE7 on Vista. For the address bar color indicators to appear in IE7 on XP, the Phishing Filter must be activated. The Phishing Filter is a recommended option during the installation routine for IE7 on XP.



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:

Enabling the Phishing Filter in IE7 (as recommended during installation) automatically enables display of the Extended Validation SSL interface and other certificate validation indicators.

VALIDATING THE CERTIFICATE AUTHORITY

To help ensure the integrity of the EV SSL Certificate authentication requirements, the CA/Browser Forum created a new independent WebTrust audit process specifically for the EV standard. All CAs who wish to issue EV SSL Certificates must pass an annual WebTrust audit confirming that the CA adheres to all EV process guidelines (as published by the CA/Browser Forum) appropriately. If a WebTrust audit discovers that a CA has issued erroneous EV SSL

Certificates or if the CA fails their WebTrust audit for any reason, that CA's root may lose its EV status in browser manufacturers' Trusted Root Store. If this happens, none of the EV SSL Certificates issued by this CA (past or present) will trigger the green address bar or the security status bar. Instead, these certificates will be downgraded to a traditional SSL Certificate and site visitors will no longer recognize the site as being authenticated pursuant to the EV guidelines.

VALIDATING A WEB SITE'S IDENTITY AND GETTING AN EV SSL CERTIFICATE

The key to the elite status of EV SSL Certificates lies in the new standard for identity authentication. In order to obtain an EV SSL Certificate, an organization must pass a strict set of requirements. For a legally-registered organization these requirements shouldn't be difficult to meet but a fraudulent operation should find them difficult to simulate. After working for over a year to hammer out the specifics, the CA/Browser Forum published the initial version of the EV guidelines on their web site in late 2006. Government agencies, corporations, general partnerships, unincorporated associations and sole proprietorships are eligible for EV SSL Certificates as long as they are currently registered with and approved by an official registration agency in their jurisdiction. Visit www.cabforum.org to read the exact text.

These guidelines specify that all identity authentication information for an organization requesting an EV SSL Certificate must originate from an authorized third-party or it must be directly verified from primary sources (such as government databases). Self-reporting is not allowed because it opens the door to unscrupulous operations who may self-submit fraudulent data. Additionally, the CA must perform an independent verification of the authority of the person requesting the EV SSL Certificate on behalf of the organization. This step makes sure that a certificate is not issued to a person not actually related to the organization that is the subject of the certificate.

The person ordering the certificate must sign an acknowledgement of agreement when placing a request for EV SSL through GeoTrust. GeoTrust must also be able to confirm the organization's registration with a government database or an official registration document must be provided.

To expedite the process or in case GeoTrust cannot verify the information elsewhere, a legal opinion letter may be submitted on behalf of the organization requesting the certificate. This letter would contain the physical address where the requesting organization performs their business, the organization's telephone number, confirmation that the organization has the exclusive right use the domain, and the employment status and authority of the individual placing the order on behalf of the organization. Furthermore, if the company has been in operation for less than 3 years, GeoTrust will require some additional confirmation of the organization's existence.

The CA/Browser Forum mandates these application requirements for EV SSL Certificates. Experienced GeoTrust sales support experts will help customers through this process. Our goal is to make the application process as streamlined as possible while maintaining high standards for quality and compliance.

EV UPGRADER ENABLES THE EV USER INTERFACE

One of the safety checks inherent in SSL is the requirement for the client browser to recognize and confirm that the root in an SSL Certificate is valid and trusted by the browser manufacturer. Every GeoTrust EV SSL Certificate is signed by two roots; a traditional SSL root and an EV root so that older systems that are unable to recognize the EV root will still recognize the traditional SSL root and will initiate a protected SSL session. If the certificate is recognized this way, the user interface will display the certificate as if it were a traditional SSL Certificate with only the padlock icon.

Windows Vista automatically updates the root store in IE7 clients on a scheduled basis, so all Vista clients should recognize the new EV SSL Certificates and will display the distinctive EV user interface green address bar. Windows XP handles root updates to IE7 clients a little differently. These systems rely on a dynamic update process that is triggered whenever the client system is exposed to a certificate signed by an unknown root. When this occurs, the XP client system will reach out to a Microsoft Root Store and look for the matching root. If one exists, the client will download that root to its local root store and the next time the client system sees that type of certificate, it will recognize it. This occurs very quickly, so that the browser will display the certificate's EV status the next time the client browser window refreshes or when the user clicks to the next page secured by the same EV root.

EV Upgrader™, embedded in the GeoTrust True Site® Seal, automatically prompts client XP systems to update their local root store with the GeoTrust EV root. An IE7 XP client need only visit a page with the GeoTrust True Site Seal once; thereafter that client will always display the EV green address bar interface whenever it encounters a web page signed with a GeoTrust EV SSL Certificate. Without EV Upgrader, IE7 on XP clients ordinarily will only display the EV Certificate as if it were a traditional SSL Certificate with only the padlock icon.

To install EV Upgrader, an organization need only install the GeoTrust True Site Seal on their web site. GeoTrust recommends installing the seal on the home page or on a page immediately preceding the first instance of an SSL secured page in the user experience. This way, all IE7 XP clients will get the full effect of the EV Certificate the first time they encounter it. For more information about EV Upgrader, refer to the GeoTrust white paper *Extended Validation SSL with EV Upgrader*.

CONSUMER CONFIDENCE: BOOSTED BY EV

Research indicates the new EV user interface boosts consumer confidence and makes online shoppers more inclined to complete web transactions.

According to an independent study in 2007 by Tec-Ed, online shoppers who were shown to EV SSL secured web sites showed improved awareness of site security, increased trust in that site, stronger feelings of site loyalty, and suspicion of a site if it did not show the EV user interface. Tec-Ed reported the following results.

- **Awareness: 100%** of survey participants expected to notice whether or not a site displays the green EV bar.
- **Trust: 97%** of survey participants said that they would be more comfortable sharing personal and financial data with sites displaying the green EV bar.
- **Loyalty: 98%** of survey participants prefer to shop in sites with the green EV bar.
- **Security Savvy: 77%** of survey participants would hesitate to shop at a site that lost its green EV address bar.

Given the strong effect of EV SSL on the user experience and the rapid adoption of EV compatible browsers by consumers, smart web sites should choose to upgrade to EV SSL Certificates. If your web site depends on collecting sensitive personal information or financial data from customers, consider getting the consumer confidence boost of an Extended Validation SSL Certificate from GeoTrust.

For more information, contact us at (800) 944-0492 or visit www.geotrust.com.