Extended Validation SSL Certificates: A Standard for Trust

THAWTE IS A LEADING GLOBAL PROVIDER OF SSL CERTIFICATES

Extended Validation SSL Certificates: A Standard for Trust

Many consumers have reservations about trusting web sites, which impacts their willingness to complete e-commerce transactions, financial transactions with their banks, and other tasks involving transmission of sensitive information. The growing frequency of web site scams – such as phishing and pharming – creates an atmosphere of fear and uncertainty.

In a 2006 report, Gartner estimates that more than 41% of U.S. adults received phishing emails, 46% changed their purchasing and online behaviors as a direct result of security concerns, and 10% reduced their online spending by at least 50%. As a result, nearly $2 billion may have been lost in sales – all due to consumer concerns over security.

When SSL was originally conceived, the Internet was a simpler place; a web site either did or did not need the encryption and authentication that an SSL digital certificate provided. Today's security needs are more granular. For example, some web sites simply need basic encryption to protect site user names and password; other sites need to handle extremely sensitive personal information and need stronger encryption as well as in-depth web site owner identity verification.

Certification Authorities (CAs), such as Thawte, have refined their product offerings to meet these differing objectives. For example, web sites requiring only basic encryption and minimal identity verification can opt for a less expensive, rapidly issued **Thawte® SSL123 Certificate** domain validation certificate. At the other end of the spectrum, Thawte offers the highly-trusted **Extended Validation (EV) SSL certificate** for web sites that handle extremely personal and sensitive data.

The EV certificate standard was developed by the CA/Browser Forum, an independent industry group, which also developed auditing guidelines to define and control the procedures used to validate and issue these certificates. When an EV certificate is in use, web browsers provide enhanced visual cues, making it clearer for consumers to determine with whom they are dealing, and whether the connection is secure. The latest version of every major web browser supports EV certificates, and most top e-commerce and banking web sites rely on EV certificates to more effectively achieve a higher level of trust from their customers.

Who Do You Trust?

The two primary purposes of an SSL certificate are to:

- Authenticate that a company's web site is valid
- Encrypt communications between the web server and the customer's web browser

Any digital certificate – with its public and private key pair – could conceivably be used to achieve encryption. The trust aspect of an SSL certificate comes from the identity verification procedures used by the CA that issues the certificate. It is the CA's responsibility to determine who actually owns the domain for which the SSL certificate will be used, and to ensure that the site owner is a legitimate business entity worthy of trust. An SSL connection should, then, help consumers develop trust: When on a phishing web site (a malicious site that masquerades as a legitimate site), consumers would not be able to establish an SSL connection, or would be able to examine the SSL certificate and see that the business they were dealing with is not the one they expected. However, traditional SSL certificates have, over time, fallen short of meeting these requirements in certain situations.

The Problems with Traditional SSL

It has always been relatively easy to counterfeit an online business. In 1995, when SSL certificates were created, web scams were few and far between. A traditional SSL certificate provided the security and reassurance people needed. There were few, if any, web sites attempting to deliberately counterfeit legitimate business web sites. Simply having the lock icon appear in your web browser – a sign that an SSL connection had been created – was enough reassurance for most consumers.

Times have changed. Web scams are more sophisticated, and scammers often obtain SSL certificates that include only validation of the web site domain name – not the identity of the

scammers or their business. As a result, counterfeit web sites can offer consumers an SSL connection, limited as it might be. Consumers see the lock icon, believe the site is legitimate, and proceed in using the counterfeit site. Consumers could examine the certificate from within their browser, but few users are technically sophisticated enough to realize that they should do so.

Some scammers even obtain full SSL certificates from less stringent CAs, meaning the scammers can obtain digital certificates attesting to an incorrect identity. In these instances, even a knowledgeable consumer who examines the SSL certificate presented by the site might well be fooled. EV certificates seek to address and resolve this problem.

EV SSL

Because EV is a joint effort between CAs and browser vendors, it offers two distinct advantages over traditional SSL certificates:

- The EV browser does a better job of raising certificate visibility within the browser's user interface (UI)
- The CAs permitted to issue EV certificates conduct more thorough identity verification of certificate requestors

The CA/Browser Forum consists of more than 20 browser manufacturers, CAs, and WebTrust authors along with the American Bar Association's Information Security Committee (ABA-ISC). The standard is under continual development to help combat evolving forms of online fraud. The EV certificate issuance guidelines define a set of best practices and standards that must be followed by CAs who issue EV certificates, and CAs must pass regular, independent audits of their processes to prove that they follow those guidelines and are worthy of issuing EV SSL certificates.

Technologically, an EV certificate functions like a traditional SSL certificate, even in older browsers that do not explicitly support the EV standard. Newer browsers, however, recognize key elements of the EV certificate, which permits those browsers to display extended UI cues that bring critical security and trust information to the forefront of the user experience.

User Experience Improvements

A key aspect of the EV standard is enabling web browsers to do a better job of communicating identity and trust-related information to the end user. The EV standard details a number of best practices to help improve the user experience.

GREEN MEANS TRUSTED

Chief amongst the user experience improvements is the guideline that EV certificates visually change the browser's address bar in some way, utilizing the color green – globally recognized as a "safe" or "proceed" color – to indicate the presence of a valid EV certificate. Different browsers implement this guideline in different ways, but all utilize the color green. All display the business name, not the web site domain name, of the entity to which the EV certificate was issued (see Figure 1). Browsers may also toggle the business name with the name of the CA who issued the EV certificate, clearly communicating to web users the company who is attesting to the business' identity.

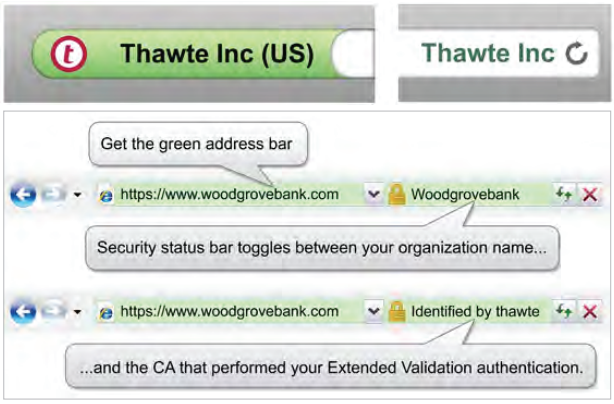

Figure 1: Visual cues enable users to recognize an EV certificate is in use.

Counterfeit web sites can not display the green address bar when using a traditional SSL certificate, and a counterfeit web site would be unable to obtain a valid EV certificate for the spoofed business due to the extended identity verification procedures required to obtain such a certificate. Although a scammer could try to deceive users by obtaining an EV certificate for their own business, the green address bar would display that business name, creating a visual mismatch between the address bar and the counterfeit web site that would tip off users to the scam.

REAL-TIME VALIDITY CHECKING

Nearly all web browsers support the use of the Online Certificate Status Protocol (OCSP) to enable real-time checks of EV certificate validity. OCSP allows a browser to check directly with the EV certificate's issuing CA to confirm the validity of the EV certificate. This is done entirely online and almost instantly when the browser is first presented with the EV certificate. Real-time checking ensures that the EV certificate has not been revoked since its issuance, and provides an extra level of security. Browsers will not display the green address bar elements unless the certificate passes this real-time validity check. Most modern

web browsers enable this functionality automatically when their anti-phishing features are enabled (see Figure 2).

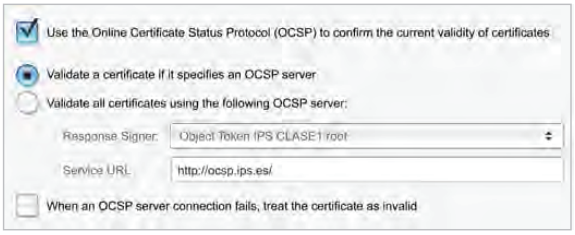

Figure 2: Enable OCSP to ensure real-time checks of EV certificate validity

EV UPGRADER™ FOR WINDOWS XP

An enormous number of computers continue to run Microsoft Windows XP with Internet Explorer 7 (IE7). Users of these computers may need to upgrade their computers' root digital certificate store in order to obtain the benefits of EV certificates and enable IE7 and later to display the appropriate EV visual cues. Thawte helps users with this by providing the free EV Upgrader™, a method for automatically updating IE7 on Windows XP clients.

The EV Upgrader can be installed as part of your web site, along with your EV certificate. The Upgrader triggers built-in Windows XP functions, and should normally be invisible to end users. After users have visited a site that includes the EV Upgrader, their IE7 web browser will automatically display the EV interface conventions when visiting a site protected with a Thawte EV SSL certificate.

Thawte makes it easy to include the EV Upgrader in your web site; it is integrated with the Thawte® Trusted Site Seal. Simply include the seal on your web page, and every Windows XP client running IE7 will automatically upgrade to EV capabilities when they visit your site.

EV SSL Solutions from Thawte

EV SSL certificates from Thawte include 256-bit, 128-bit, 56-bit, and 40-bit encryption, supporting a wide range of web browsers. Browsers automatically select the highest level of encryption they are capable of using. Thawte EV certificates are fully compliant with the CA/Browser Forum's guidelines and requirements, and Thawte passes regular audits to ensure this compliance.

Useful Links

You may find the following URLs to be useful:

- Learn more about Thawte EV certificates and initiate an EV certificate purchase at: https://www.thawte.com/ssl-digital-certificates/extended-validation-ssl-ev/index.html
- Read about Thawte's EV FAQs at: http://www.thawte.com/resources/ssl-information-center/inspire-trust-online/extended-validation-ssl-faq/index.html

To learn more, contact our sales advisors:

- **Via phone**
  - **US toll-free: +1 888 484 2983**
  - **UK: +44 203 450 5486**
  - **South Africa: +27 21 819 2800**
  - **Germany: +49 69 3807 89081**
  - **France: +33 1 57 32 42 68**
- **Email sales@thawte.com**
- **Visit our website at https://www.thawte.com/log-in**

Protect your business and translate trust to your customers with high-assurance digital certificates from Thawte, the world's first international specialist in online security. Backed by a 17-year track record of stability and reliability, a proven infrastructure, and world-class customer support, Thawte is the international partner of choice for businesses worldwide.