

Protecting Your Name on the Internet

The Business Benefits of Extended Validation SSL Certificates



Contents

1. Where We Are Now.....	3
2. How SSL Certificates Work.....	3
3. Cracks in the System	4
4. A Solution.....	4
5. Impacts on Businesses.....	5
6. Conclusion.....	5



1. Where We Are Now

By the mid-2000s the standard Internet browser trust model was in need of an upgrade. While it had served the community well since its inception by Netscape in the mid-1990s, protecting trillions of dollars of e-commerce, it was not able to stand up to the modern threats posed by phishers and spoofers on the Internet.

The browser trust model, which is based on Secure Sockets Layer (SSL) certificates, uses cryptographic protocols which provide secure communications for such things as web browsing, email, instant messaging, and online e-commerce. A Web site with an SSL certificate could be easily identified by a gold padlock icon in the address bar. If the site's certificate was issued by a Certificate Authority whose root key was installed in the browser, the lock would show as closed. If it was not, or the certificate name did not match the domain name, the lock would remain open, indicating to the user that this site was not secure. This gave the consumer a degree of trust that the Web site they were visiting was legitimate and had security in place to protect their information. Online e-commerce has never looked back.

2. How SSL Certificates Work

SSL certificates are based on public-key cryptography. Public-key cryptography is a form of cryptography where there are two separate keys, a public key and a private key. The public key can be widely distributed, but the private key is kept secret. The keys are related mathematically, but the private key cannot be compromised from the public key. Items encrypted with a public key can only be decrypted with the corresponding private key. Private keys are encrypted and protected with passphrases that only the key holder would know.

From an SSL certificate standpoint, the public key is placed into an electronic document, referred to as a certificate. That certificate is then signed by a trusted Certificate Authority (CA), such as Go Daddy. The CA performs reasonable investigation to assure that the certificate requestor is the controller of the domain name for which the certificate is being requested. Once this is completed, the CA issues an SSL certificate for the requested domain name. The SSL certificate is installed on the Web server of the domain for which it was issued. When users connect to the SSL protected Web server, their browser requests a secure connection. The Web server sends its identification to the user's browser in the form of a digital certificate. This certificate consists of the server name (or company name), the trusted CA, and the server's public encryption key. The user's browser encrypts the information for transit to the Web server so that only the SSL certificate holder can decrypt it with its private key.



3. Cracks in the System

This model was very effective for the first decade of Internet e-commerce, but as time went on, malicious parties became savvier in their ability to spoof the system and exploit it. These people became known as spoofers. Spoofers secured many popular and commonly misspelled domain names and took advantage of users' mistakes for their criminal activity.

Most CAs checked a business' credentials before issuing a certificate. However, because no standard existed for CAs to verify the identity of the business, there were some discrepancies in the level of verification applied to certificate requests. As a result, the identity aspect of SSL certificates has been abused.

The importance of the gold padlock signifying an SSL-secured website is still important. However, without verified site identity information, users could be sending personal information to the wrong Web site, resulting in identity theft. Over time, and after many large-scale media stories about compromises in seemingly secure Web browsing resulting in identity theft, consumer confidence in secure e-commerce began to wane. It should be noted however, that the technology of SSL certificates was not compromised at any time; rather, the issuance of the certificates to fraudulent domain holders caused the issues.

4. A Solution

In 2005 the CA/Browser Forum, a voluntary organization of leading certification authorities and Internet browser software vendors, was founded. This group created a set of guidelines for a new type of SSL Certificate which was named the Extended Validation (EV) certificate. They also created standardized procedures for verifying and ensuring the identity of the EV certificate holder. These new EV certificates offer highly rigorous checks before being issued and are still fully backwards compatible with older browsers. They became widely available in 2007.



EV SSL certificates immediately became a very useful tool to companies conducting online commerce as a way to protect their name and brand image from phishers and spoofers. These new EV certificates have a visible impact on the user's browsing experience by showing a green background behind the address bar for sites that are protected by an EV SSL Certificate in Microsoft Internet Explorer 7.

A similar visual indicator has been introduced in Firefox 3, although every browser may implement their own EV user interface. These visual indicators offer an immediate and unique way to show consumers that the site they are visiting has gone through the rigorous checks required to have an EV SSL Certificate.

5. Impacts on Businesses

Current Go Daddy SSL certificate customers can upgrade to the new EV certificate at any time with little impact on their current certificate installation procedures.

New EV certificate customers will have to provide more information to us than they would have with the previous process before the new certificate can be issued. But, they can rest assured that they are doing the most they can to ensure customer comfort while doing business on their Web site.

6. Conclusion

With e-commerce quickly becoming a major factor in the world economy, customers' private information must be secured. The new EV SSL certificates are a huge step forward both in the consumer confidence arena and in the spirit of cooperation between CAs to ensure the security of users' data.

Sites with EV SSL certificates will show a green background behind the address in the Web browser. Web sites without EV SSL certificates will continue to show the white background currently used. Sites with invalid certificates or sites that are known to be fraudulent or malicious will display in red.

As Web browsers with the new SSL display technology become more prevalent in the wild, the interface changes noting EV certificates will become more accepted, and expected from companies doing business online. Before long, the green address bar will be synonymous with "this is secure".



An Extended Validation SSL Certificate helps e-commerce site visitors complete secure transactions with confidence and puts these sites in a leadership position. If one site has the “green bar” in the browser and another site does not, the site with the “green bar” will appear to be more trusted and more legitimate.

For more information on Go Daddy’s SSL certificate options visit <http://www.godaddy.com/gdshop/ssl/ssl.asp>

