



Foundation Repair: Extended Validation SSL

A New Model for SSL Certificates and Browser Trust

July 2009

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. Entrust is a registered trademark of Entrust Limited in Canada. All other company and product names are trademarks or registered trademarks of their respective owners. The material provided in this document is for information purposes only. It is not intended to be advice. You should not act or abstain from acting based upon such information without first consulting a professional. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

© 2009 Entrust. All rights reserved.

Table of Contents

1	A New Model.....	1
2	SSL, Certificates Primed the E-Commerce Pump	1
3	Cracks Appearing In the Browser Trust Model	1
4	What Is Being Done to Fix Browser Trust?.....	2
5	SSL Certificates Before Extended Validation	2
6	Impact of Extended Validation SSL Certificates.....	3
7	The Myth of Server-Gated Cryptography (SGC).....	5
8	Extended Validation Is a Reality	6
9	What Can I Do Now?	6
10	About Entrust	6

1 A New Model

In 2005, the longstanding Internet browser trust model, which had served as a foundation for many billions of dollars of e-commerce, was starting to show signs of age. Just like an older building, the model was in need of renovation and repair to its foundation in order to ensure it could continue to support future e-commerce initiatives.

Based on Secure Sockets Layer (SSL), certificates and the ubiquitous padlock icon, the browser trust model was reworked to help renew consumer confidence and to better suit handling e-commerce transaction volumes as they continued to increase.

The new model was defined by a group called the CA/Browser Forum, and consumers first saw the results of their work in January 2007. This paper outlines why the group was formed, what it is working toward and the impact it has on consumers and Web site operators.

2 SSL, Certificates Primed the E-Commerce Pump

In the mid 1990s, Netscape foresaw the need for security to enable the adoption and growth of e-commerce. Creating and embedding the SSL security protocol in their browser and server products was the first step, but the real challenge was building consumer trust.

From the outset, a key or padlock icon was chosen to represent a secure SSL connection, and consumers were told that if the lock was closed, they were dealing with a “trusted” Web site.

Whether a site was trusted or not was based on the digital certificate it presented to the browser through SSL. If the server certificate was issued from a certification authority (CA) whose root key was embedded in the browser, then the lock would immediately close. A decade and many billions of dollars in e-commerce later, the lock icon has served its purpose well.

3 Cracks Appearing In the Browser Trust Model

While SSL and the padlock icon have served as a solid foundation for many years, some cracks are appearing. Con artists always have searched for ways to exploit the learned responses of their fellow humans and the Internet has brought with it many new opportunities. With varying degrees of sophistication, examples have appeared where consumer trust of the lock icon has been abused.

In one exploit, a server certificate was acquired under false pretenses to give a phishing Web site extra credibility as it attempted to steal usernames and passwords.¹ In other potential exploits, fake lock icons are embedded directly in the Web pages using simple graphics or more sophisticated active code to lull users into a false sense of security.

¹ [“The New Face of Phishing,” The Washington Post, Brian Krebs, February 2006](#)

4 What Is Being Done to Fix Browser Trust?

To bolster consumer trust in the foundation of e-commerce before it is irreparably damaged, several CAs and browser vendors have come together to establish a higher security approach based on common standards. The CA/Browser Forum has created a new tier of SSL certificate with very high standards for validation and assurance, and is also exploring browser security user-interface elements (e.g. colors, padlock location) and behavior.

The new certificates were referred to by different names as they were being defined — “High Assurance” and “Enhanced Validation” were considered — but “Extended Validation” was the final name chosen by the CA/Browser Forum. It is important to note that these certificates are still fully compliant with the X.509 standards and are backwards compatible with older browsers.

Now that these new validation processes are in place, all CAs will use the same highly rigorous checks before issuing one of these new SSL certificates, and browsers detecting one of these certificates at a Web site can reflect the higher trust level in the user interface.

5 SSL Certificates Before Extended Validation

Using certificates in SSL is based on public key cryptography. This paper won't attempt to explain public key technology in detail, but at a high level the Web server needs to create a mathematically related pair of keys — the private key and the public key. The public key portion of the pair is then put into an electronic document called a certificate and signed by a trusted CA.

For SSL server certificates it is important that the Web server's domain name (e.g., www.company.com) be present in the certificate, otherwise browsers will warn users that they may not be on a legitimate site.

From a human perspective, the Web server administrator begins this process by issuing commands in the Web server to generate the keys and to create a “Certificate Signing Request,” or CSR. The administrator then submits the CSR to the CA, generally submitting it through a Web page. Workflow then begins at the CA to validate that the certificate can be issued as requested.

Before Extended Validation, requirements varied significantly between CAs, without an easy way for consumers to distinguish certificates issued using more- or less-rigorous validation processes.

Some CAs still are willing to issue certificates after simply checking that the requestor controls the domain name requested. This is accomplished by sending an automated e-mail to the administrator e-mail address listed in the Internet registry for the requested domain name.

What's in a name?

The purpose of a certificate is to assign a key to an individual key-holder's name. There are many forms of name in common use. Some are unique, and others are shared. Some are meaningful, and others are meaningless. By virtue of the way they are assigned, domain names are unique but meaningless.

Certificates that bind a key only to a domain name do offer some protection against such attacks as HTTP response-splitting and ISP eavesdropping. However, these are relatively uncommon. The most prevalent type of attack today, of course, is phishing. Domain name-only certificates offer little or no protection against this type of attack.

The approach is very fast and convenient for both CA and for customers, but it introduces some risk in that spoofers can register a domain that looks very similar to a target domain. Harvard researchers demonstrated this risk and documented their findings.²

Most CAs will check a business's credentials in more detail before issuing a certificate, but there are discrepancies in the level of rigor applied. Some CAs simply accept faxed copies of a company's utility bill.

Other CAs, like Entrust, have been more rigorous from the outset and will not accept information provided by the requestor at face value, instead looking up company registration information in trusted databases. They also will typically verify that the individual requesting the certificate is properly authorized by the organization by initiating phone calls to listed numbers for the company.

This inconsistency of validation processes between CA vendors was one of the key focus issues for the CA/Browser Forum.

6 Impact of Extended Validation SSL Certificates

Extended Validation SSL certificates have the highest impact on consumers, reassuring them that the site they are visiting is legitimate through visual cues in un-modifiable parts of the browser interface "chrome." For example, Microsoft Internet Explorer Version 7 (IE 7), Mozilla's Firefox 3 and Opera 9.5 display the corporate name with a green background for sites protected by an Extended Validation SSL certificate.

IE 7 highlights the entire address bar in green and displays the name of the CA (e.g., Entrust) in a scrolling user interface (UI) element beside a more prominent padlock icon. Sites without Extended Validation SSL certificates simply have an address bar with a white background.

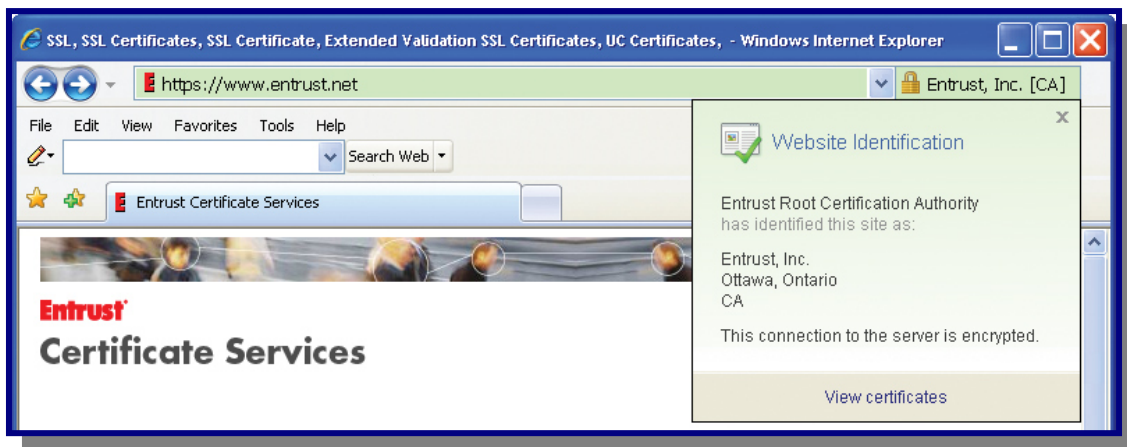


Image 1: Microsoft Internet Explorer 7 visiting an EV-enabled Web site

² Source: http://people.deas.harvard.edu/~rachna/papers/why_phishing_works.pdf

It is expected that these prominent UI changes will become widely accepted and expected by consumers, providing organizations with a new tool to demonstrate to customers that they take security and privacy seriously.

Web site operators will notice differences in the amount of information they need to provide to CAs during the initial validation process. Although certificate validity periods are now limited to two years, Web site operators using these certificates may notice that their information is revalidated by their CA after 12 months.

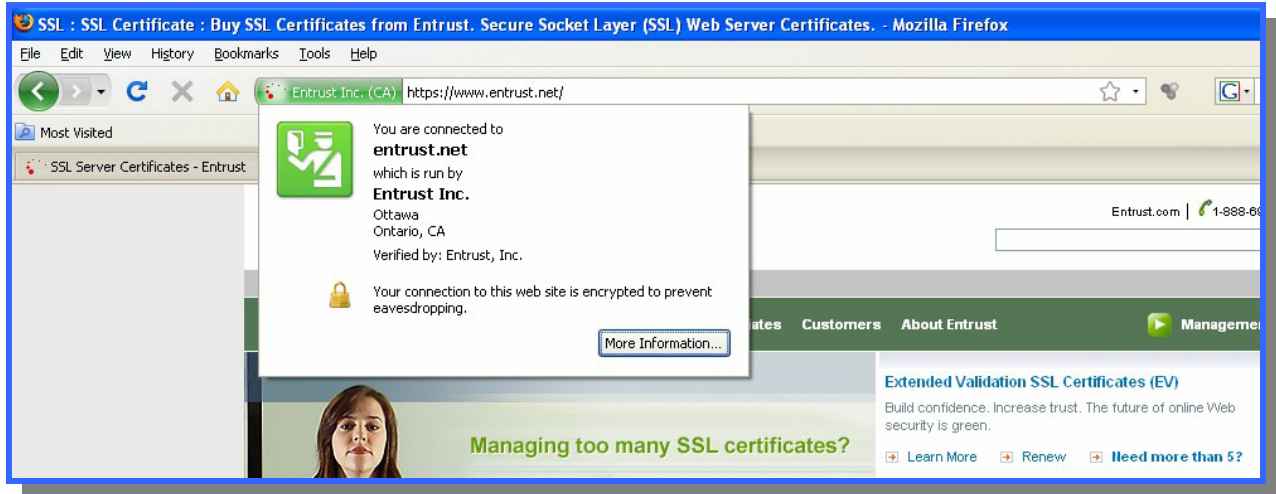


Image 2: Firefox 3 visiting an EV-enabled Web site

Wildcard certificates are no longer acceptable, and for deployments with requirements to protect multiple hostnames with a single certificate, each hostname will need to be included in the certificate using multiple “subjectAltName” attributes.

Certificate revocation checking will be active by default in many new browsers. This will allow a CA to react to a problem by revoking a certificate that, in turn, enables browsers to detect if a certificate is no longer trustworthy. Past versions of browsers have been inconsistent in their implementations and default settings for revocation checking.

7 The Myth of Server-Gated Cryptography (SGC)

Whether they are standard or EV certificates, SSL certificates should support 128- or 256-bit security for confidentiality of information traveling over the Internet. This means that the secure session between a browser and server is encrypted with a 128- or 256-bit key to prevent information from being intercepted and decoded. SSL certificates from Entrust support both 128- and 256-bit security.

Even today, some vendors imply that 128-bit security requires support of "Server-Gated Cryptography" (SGC) and sell these certificates at a significant premium. SGC is not required to enable 128-bit security for virtually all browsers deployed today; they even can introduce serious security threats.

According to industry statistics, more than 99.6 percent of browsers in use today support either 128- or 256-bit encryption without SGC³. For the few users with these older browsers, converting is straightforward with upgrade packs available for most browsers. For this reason, premium-priced "step-up" Web server certificates are no longer necessary.

More importantly, for the security of organizations and their end-users, older versions of browsers that do require SGC — sometimes referred to as "export-strength" or 40-bit browsers — can represent increased security vulnerability.

For example, Microsoft Internet Explorer version 5.0.1 — only used by 0.06 percent⁴ of the population — was the last IE version requiring SGC for 128-bit operation; a longstanding update has been available on Microsoft Windows Update to bring it up to 128-bit encryption. As such, most users who still require SGC are using a Web browser that has not had security updates to address the multitude of other security issues identified. This poses a significant risk to both the user and the organization.

EV certificates alone are superior to SGC certificates or a combination of EV with SGC certificates. Why? EV certificates require the end-user to use a browser protected by at least 128-bit encryption for SSL security. This requirement ensures the consumer is using a relatively up-to-date browser (eliminating the need for SGC), thus making the user's Internet session, as well as the organization using the EV SSL certificate, more secure from the onset.



³ ["Browser Version By Market Share," August 2008, Net Applications](#)

⁴ [Ibid.](#)

8 Extended Validation Is a Reality

The CA/Browser Forum was formed in May 2005 and has been driving toward consensus since that first meeting. Efforts to extend the scope of Extended Validation SSL certificates are continuing, but the value of Extended Validation SSL certificates is a reality today for users of Microsoft's Internet Explorer 7 browser — estimated at almost 46.7 percent⁵ of the browsers in use — Mozilla's Firefox 3 and Opera 9.5. Entrust Extended Validation SSL certificates have been available since January 2007.

9 What Can I Do Now?

Entrust customers who wish upgrade to Extended Validation SSL certificates can do so today, with minimal changes to their existing procedures. Customers using large numbers of Extended Validation SSL certificates should consider switching to the Entrust Certificate Management Service in order to benefit from streamlined validation and the flexibility of the subscription approach to certificates.

For the latest information on this topic, please visit www.entrust.net/ev.

10 About Entrust

Entrust provides trusted solutions that secure digital identities and information for enterprises and governments in 2,000 organizations spanning 60 countries. Offering trusted security for less, Entrust solutions represent the right balance between affordability, expertise and service. These include SSL, strong authentication, fraud detection, digital certificates and PKI. For information, call 888-690-2424, e-mail entrust@entrust.com or visit www.entrust.com.

⁵ ["Browser Version By Market Share," August 2008, Net Applications](#)