



A Proper Foundation: Extended Validation SSL

*A critical model for SSL digital certificates
and browser trust*

Get this
White Paper





Contents

Context of Internet Security	3
Early Growth	3
Trust Model Weakness	3
Creation of Extended Validation	4
What's in a Name?.....	4
EV Adoption	4
SSL Certificate Primer	5
Impact of Extended Validation SSL Certificates.....	6
Browser Vendor Education	8
Google.....	8
Mozilla	9
Apple	9
The Myth of Server-Gated Cryptography (SGC)	10
What Can I Do Now?	11
Entrust & You	12



Context of Internet Security

In 2005, the longstanding Internet browser trust model, which had served as a foundation for many billions of dollars of ecommerce, 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 ecommerce 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 ecommerce 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.

Early Growth

In the mid-1990s, Netscape foresaw the need for security to enable the adoption and growth of ecommerce. 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” website.

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 ecommerce later, the lock icon has served its purpose well.

Trust Model Weakness

While SSL and the padlock icon served as a solid foundation for many years, cracks were appearing. Con artists always have searched for ways to exploit the learned responses of their fellow humans. 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 website extra credibility as it attempted to steal usernames and passwords. In another exploit, an SSL renegotiation vulnerability was used to hack a popular social media site.¹

¹ “Researcher Hacks Twitter Using SSL Vulnerability,” Brian Prince, eWeek, November 16, 2009.

“

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.

”



Creation of Extended Validation

To bolster consumer trust in the foundation of ecommerce before it was irreparably damaged, several CAs and browser vendors came together to establish a higher security approach based on common standards.

The CA/Browser Forum created an advanced tier of SSL certificate with very high standards for validation and assurance, but also added more obvious 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 website can reflect the higher trust level in the user interface.

EV Adoption

Looking at the top-20 Web browser versions in use today (e.g., Microsoft IE 7.0+, Google Chrome 17+, Apple Safari 5.0+, Mozilla Firefox 4+ and Opera 11+) more than 86 percent of the market is EV-capable.² This signifies remarkable adoption — by end-users, CAs and browser developers alike — in a relatively short timeframe.

The remaining seven percent of browser versions outside the top-20 also likely support EV SSL as well, but each has a current market penetration of 0.36 percent or less.

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-validated (DV) certificates offer little or no protection against this type of attack.

² “Desktop Browser Version Market Share,” NetMarketShare, Net Applications, August 2012.



SSL Certificate Primer

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.

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.

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.



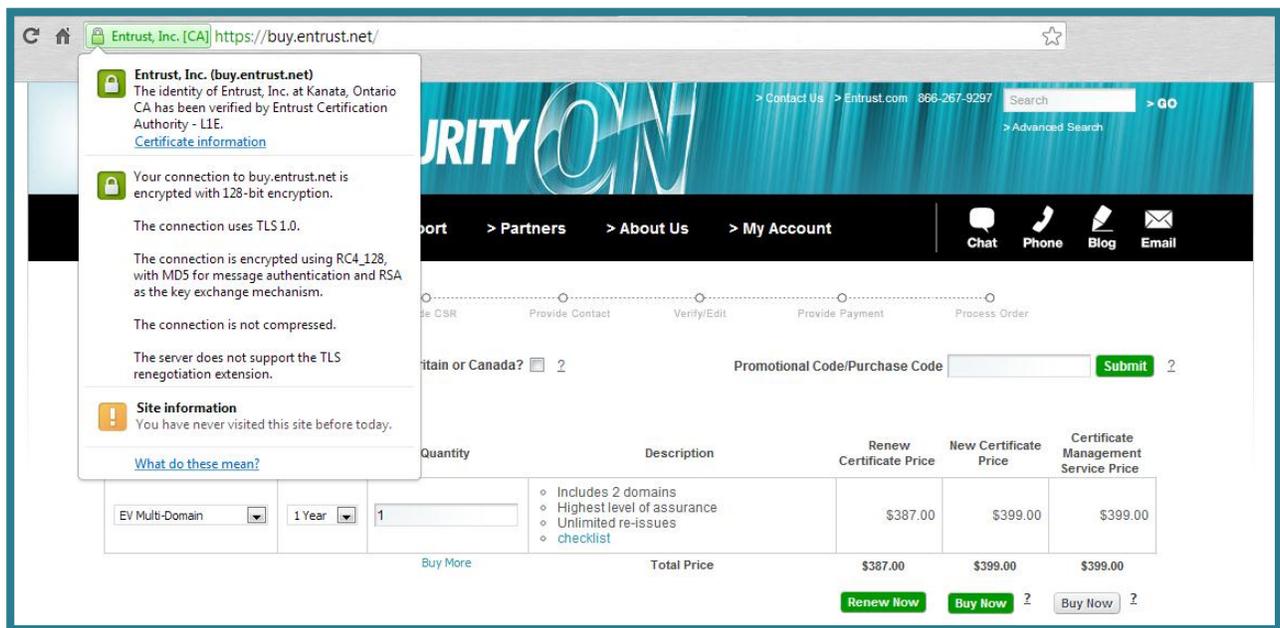


Impact of Extended Validation SSL Certificates

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, the latest versions of Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, Opera and Apple Safari display the corporate name with a green background for sites protected by an Extended Validation SSL certificate.

In different manners, all highlight the entire address bar in green and displays the name of the CA (e.g., Entrust, Inc.) 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.

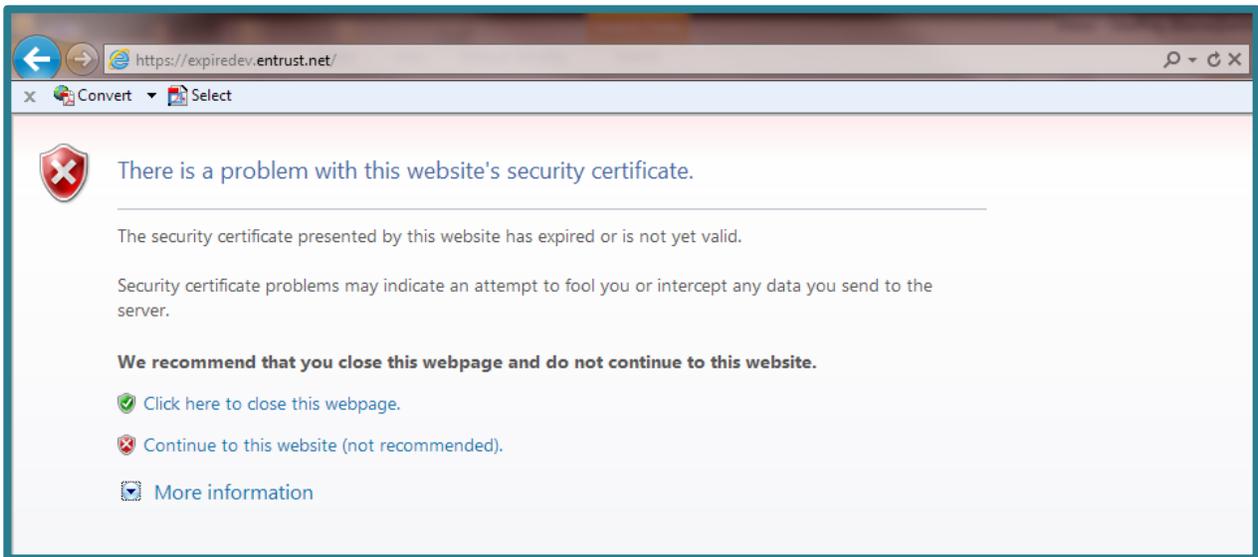


Google Chrome visiting a verified EV-enabled website, which gives detailed information about existing encryption, issuing certification authority (CA) and cryptography in use.



These prominent UI changes are widely accepted and expected by consumers, providing organizations with a proven tool to demonstrate to customers that they take security and privacy seriously.

Website 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, website operators using these certificates may notice that their information is revalidated by their CA after 12 months.



Microsoft Internet Explorer 9 visiting a site with an expired EV SSL certificate. A red "X" alerts the user that there is a critical issue with the installed certificate. The notification provides a recommendation on how to proceed and an option to view additional information.



Browser Vendor Education

Many of the more responsive browser vendors are doing their best to educate consumers on the benefits of SSL and EV SSL and how the technology will protect transactions and communication online.

Google

Google, for example, provides an easy-to-understand³ primer on browser and SSL security, as well as what the different elements of SSL communicate. Part of this includes a clear explanation⁴ of what different browser icons mean.

Google: Website Security Indicators

Icon	What it means
	The site isn't using SSL. This icon displays for http:// sites. Most sites don't need to use SSL because they don't handle sensitive information. Avoid entering sensitive information, such as your credit card information or bank login information, on the page. If sensitive information is being requested on a site not using SSL, consider contacting the website owner.
	Google Chrome has successfully established a secure connection with the site. Look for this icon and make sure the URL has the correct domain, if you're required to log in to the site or enter sensitive information on the page. If a site uses an Extended Validation SSL (EV-SSL) certificate, the organization's name also appears next to the icon in green text.
	The site uses SSL, but Google Chrome has detected insecure content on the page. Be careful if you're entering sensitive information on this page. Insecure content can provide a loophole for someone to change the look of the page.
	The site uses SSL, but Google Chrome has detected either high-risk insecure content on the page or problems with the site's certificate. Don't enter sensitive information on this page. Invalid certificate or other serious https issues could indicate that someone is attempting to tamper with your connection to the site.

³ "Privacy and security settings," Chrome Help, Google.

⁴ "Website security indicators," Chrome Help, Google.



Mozilla

Like Google, Mozilla, makers of the popular Firefox browser, provide step-by-step instructions⁵ about the different browser security elements. From a “gray globe” to “green padlocks,” this consumer education is important for building general SSL trust.

Apple

Apple, who creates Apple Safari for OS X, offers a “Security and Privacy” section on their website⁶ that serves as a comprehensive list of all the browser’s security abilities.

And while they offer a specific section on EV certificates, they also show how Safari provides an obvious “HTTPS badge” that clearly lets users know they’re on a secure site that’s using verified SSL encryption.



⁵ “How do I tell if my connection to a website is secure?” Firefox Help, Mozilla.

⁶ “Safari Features: Security and Privacy,” Apple Inc.



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 SGC⁷. 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 — basically no longer in use by the population⁸ — 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.



⁷ "Desktop Browser Version Market Share," NetMarketShare, Net Applications, August 2012.

⁸ Ibid.



What Can I Do Now?

Entrust customers who wish upgrade to Entrust Multi-Domain 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.



Entrust & You

More than ever, Entrust understands your organization's security pain points. Whether it's the protection of information, securing online customers, regulatory compliance or large-scale government projects, Entrust provides identity-based security solutions that are not only proven in real-world environments, but cost-effective in today's uncertain economic climate.

A trusted provider of identity-based security solutions, Entrust empowers governments, enterprises and financial institutions in more than 5,000 organizations spanning 85 countries.

Entrust's award-winning software authentication platforms manage today's most secure identity credentials, addressing customer pain points for cloud and mobile security, physical and logical access, citizen eID initiatives, certificate management and SSL.

For more information about Entrust products and services, call **888-690-2424**, email entrust@entrust.com or visit entrust.com.

Company Facts

Website: www.entrust.com
Employees: 359
Customers: 5,000
Offices: 10 Globally

Headquarters

Three Lincoln Centre
5430 LBJ Freeway, Suite 1250
Dallas, Texas 75240

Sales

North America: 1-888-690-2424
EMEA: +44 (0) 118 953 3000
Email: entrust@entrust.com

follow us on
 