



**KPMG ANALYSIS**

## For Better Security, Web Browsers Go Green

June 26, 2007

By Dave Pelland, Managing Editor, Digital Insider

A new generation of Web browser certificates could help restore consumer faith in e-commerce as phishing attacks hit financial services providers, retailers and other companies.

On June 12, the C/Browser Forum, a group of more than 30 certification authorities (CAs) and Web browser software vendors, released guidelines for extended validation (EV) SSL (secure sockets layer) certificates and procedures for verifying the legal entity that controls a Web site.

EV certificates, which have been under development for about two years, offer greater protection than previous methods in two major areas. An EV certificate requires a stronger validation process than traditional SSL certificates, and updated Web browsers that recognize EV certificates can indicate clearly when a transaction is secure.

"There's a large problem with identity on the Web," says Andrew Codrington, product manager for the certificate services unit of security provider Entrust. "Consumers and businesses need to be able to verify they're on the Web site they intended to be on."

The effort to develop EV certificates comes in response to phishing attacks, which try to trick consumers to enter personal information and passwords into fraudulent Web sites designed to look like legitimate bank or auction sites.

According to the Anti-Phishing Working Group, there were more than 55,600 unique phishing Web sites detected in April 2007, compared with 20,781 in March and 11,121 in April 2006. More than 92 percent of the April 2007 attacks were aimed at customers of financial services firms, with social networking and Web-based e-mail providers also being targeted.

For consumers, the most obvious change with EV certificates will be in their Web browser screen. When a secure connection is established to a site that uses an EV certificate, the browser's address bar is highlighted with a bright green background, and a small window next to the address bar displays the corporate name of the entity that has been issued the certificate, as well as the certification authority.

For sites without EV certificates, the traditional lock icon will appear within the browser window.

"We wanted a way to more visibly display the certificate in the browser, and we needed to pull content directly from the certificate," says Troy Kitch, product manager for SSL certificates for security provider VeriSign. "If you're using these high standards across all the CAs, you want to make sure that information is displayed where people can easily see it."

Online merchants hope the increased security will promote consumer confidence in

**MORE...**

**Attachment Spam May Emerge as Malware Vector**

AUGUST 8 PDF attachments are the latest effort to evade corporate spam filters, and may foreshadow the use of e-mail attachments as a way to deliver malware.

**Selected Technology Company Earnings**

JULY 31 Technology and media companies generally reported earnings growth in the second quarter.

**Transfer Pricing Risk Hitting Boardroom Agendas**

JULY 25 Technology companies face a major challenge in transfer pricing risk as national governments seek new sources of tax revenue.

**Product Placement Takes Its Role on the Global Stage**

JULY 18 The head of a television studio talks about how product placements are expanding across the globe.

**Data Protection Gets Policy, Tech Backing**

JULY 11 The focus of enterprise security is shifting to data protection and stronger policies for accessing and storing information.

**IT Governance Is a Matter of Information Over Technology**

JULY 5 A language barrier between audit committee members and technology officers can severely complicate IT risk oversight.

**Growth, Profit and Expansion in the Global Semiconductor Industry**

JUNE 18 Gary Matuszak, global line of business chair in KPMG's Information, Communications & Entertainment practice, and Ron Steger, a KPMG partner in the same practice, discuss KPMG's annual Semiconductor Survey.

online transactions. Kitch said one merchant has reported an 8.6 percent reduction in shopping cart "abandonment rates" when customers use browsers that support EV certificates.

Microsoft's Internet Explorer 7 browser recognizes EV SSL certificates, while Mozilla's Firefox and browsers from Opera Software and KDE are scheduled to have similar capabilities by the end of the year.

"When people are involved in an online transaction, they're thinking of the task at hand -- they're not always thinking about trust issues or SSL certificates," Kitch says. "If a green bar shows, that's evident and easier to see."

The need for stronger browser authentication is a result of a few certificate authorities that began issuing certificates through an automated process, which validated only that a person or organization had registered a specific domain. These "domain validation" certificates, which started hitting the Web about five years ago, were an inexpensive way to ensure that a Web transaction would be encrypted.

However, the domain validation certificates did not verify the legitimacy of a company running a Web site. If criminals registered a domain name similar to that of a financial institution and launched a phishing attack, the browser would display a secure-transaction lock icon, which in turn would increase the apparent authenticity of the fraudulent site.

"Instead of a certificate helping you identify who you're doing business with and sending your information to, domain-validated certificates only enable encryption between you and a Web site," says Mark Lundin, a senior manager in KPMG's IT Advisory practice in San Francisco.

"There are some Web sites that don't offer assurance of who operates the site, while other sites use higher assurance certificates that do," Lundin says. "But within the browser, there is no difference -- the lock would appear with both types of certificates. The lock icon once meant that the Web site operator's identity had been validated, but that's no longer the case."

To help eliminate this problem, KPMG's Lundin says CA/Browser Forum members collaborated to develop tougher standards for checking the legitimacy of a company requesting an EV certificate. For example, certification authorities are required to perform a detailed series of checks to verify the Web site operator's legal existence and identity, physical place of business, ability to engage in business, right to use the domain name and the authority of the requestor to obtain an EV certificate.

"EV SSL certificates and related browser enhancements can help companies fight phishing and demonstrate their commitment to online security, while providing an intuitive way for users to verify who they are doing business with," says Lundin.

VeriSign's Kitch says more than 1,000 Web site operators -- primarily financial services firms, travel providers and online retailers -- have purchased EV certificates.

Now that EV certificates are being adopted, the CA/Browser Forum is working with Web site operators and browser vendors to educate consumers on how EV SSL certificates work and the types of security information they'll see on their screens during secure transactions.

"It's this chicken-and-egg thing," says VeriSign's Kitch. "We wanted to make sure there were enough people with the ability to see the green bar, and then start to educate people."

To print this article or share it with a colleague, click an option below.

[Print this Article](#)

[E-Mail this Article](#)

**PLEASE RATE THIS ANALYSIS**

**Quality of Analysis**

1  2  3  4  5   
POOR EXCELLENT

**Comments or Questions**

**e-Mail Address** (optional to enable Insiders to reply)

[Submit](#)