Research Brief

Aberdeen Group
A Harte-Hanks Company

January 2011

Extended Validation SSL Server Certificates: Both End-Users and Site Owners Look Up to the Other "Green" IT

Aberdeen's June 2010 research on *Enterprise Key Management* found that users of enterprise key management solutions had substantially better results than non-users, in the critical areas of supporting greater complexity and scale of encryption at lower total cost. Perhaps one of the most overlooked areas for improved key management involves deployments of **SSL Server Certificates** and **Extended Validation (EV) SSL Server Certificates** – the latter which require a more rigorous vetting process to confirm the identity of the requesting site owner before being issued. Aberdeen's data shows that leading performers were 1.7-times more likely than lagging performers to have current deployments of EV SSL Server Certificates, providing their end-users with a higher level of assurance of a legitimate web site and greater confidence in conducting online transactions.

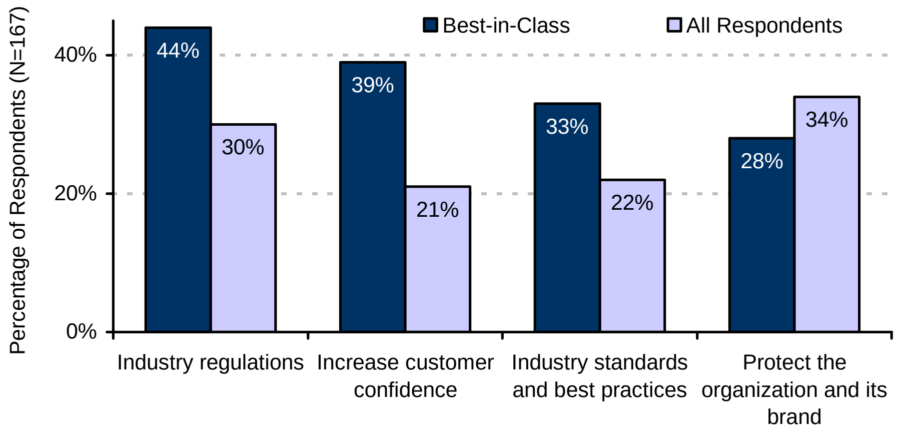
Research Brief

Aberdeen's Research Briefs provide a deeper exploration of a key finding from one or more primary research studies, including key performance indicators, Best-in-Class insight, and vendor insight.

Business Context: Securing the Online User Experience

The compelling economics of driving commerce to online channels – including reducing costs through self-service websites, providing end-users with convenient, 24-hour access to conduct transactions, and elimination of paper-based statements and mailings – are substantially diminished if end-users lack confidence in doing their business online. Ongoing end-user education continues to increase general awareness of the risks of *malware*, *phishing*, *identity theft* and never-ending mutations of *online fraud*, which in turn creates a dampening effect on their willingness to transact online.

Figure 1: Leading Pressures Driving Current Security Investments



Source: Aberdeen Group, January 2011

"We constantly strive to strike the optimal balance between leading edge security technologies on the one hand, while still providing our online customers with the access and convenience they have come to expect. We achieve this through a flexible, multi-layered approach to security."

~ Director of Customer Service, leading US bank

Not surprisingly, Aberdeen's research identifies both *increasing customer confidence* (which is about enhancing revenue) and *protecting the organization and its brand* (which is about managing risk) as leading drivers for current investments in IT Security to address these very issues (Figure 1). When examined together, these two drivers – **confidence** and **brand** – provide a concise summary of the horns of the dilemma faced by many end-user facing organizations: on the one hand, to be more open and accessible – any time, any place; and simultaneously to be more safe and secure on the other, in perception as well as in fact.

Extended Validation (EV) SSL Server Certificates, which require a more rigorous vetting process to confirm the identity of the requesting site owner before being issued, are designed to address both sides of that equation. This Research Brief looks at the role of EV SSL Server Certificates in providing end-users with a higher level of assurance of a legitimate web site, and in increasing their confidence in the security of conducting online transactions.

Differentiating SSL and Extended Validation SSL

Developed in the mid-1990s, **Secure Sockets Layer (SSL)** is now a worldwide standard technology for creating an encrypted channel between a web browser and a web server, to ensure the *privacy* and *integrity* of all data transmitted on the network for a given session. SSL Server Certificates also provide site-to-user *authentication* – i.e., SSL Server Certificates issued to organizations authenticate the organization's web site to the end-user's web browser. Virtually all web browsers in current use support SSL, and over time millions of end-users have been conditioned to recognize **https://** in their browser's address bar and the "golden padlock" that appears in their browser as visual indicators that they are viewing a secure web page.

Fast Facts

Dr. Taher Elgamal, who is credited as the inventor of SSL technology, was awarded the RSA Conference Lifetime Achievement Award in April 2009 for his contributions to the field of IT Security.

Extended Validation = A More Rigorous Issuance Process

The Extended Validation standard, developed by the **Certification Authority / Browser Forum** – a collaborative effort of more than 30 leading certification authorities and vendors of web browser software – defines "the guidelines and means of implementation for the Extended Validation SSL Certificate standard as a way of providing heightened security for Internet transactions and creating a more intuitive method of displaying secure sites to Internet users." At a high level (see www.cabforum.org for detailed information about the vetting process), requirements that must be met when requesting the issuance of an EV SSL Server Certificate include the following:

- Must be a legally recognized entity, created by an appropriate legal filing (e.g., by a certificate of incorporation), or an entity that is chartered by a state or federal regulatory agency
- Must have a registered agent or a registered office within the jurisdiction of incorporation

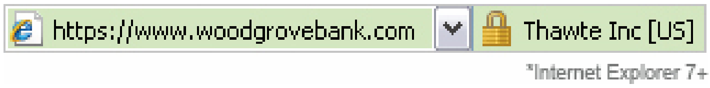
- Must not be designated as "inactive," "invalid," "not current," or the equivalent
- Must have a verifiable physical existence and business presence
- Must not be in any country where the issuer is prohibited from doing business or issuing a certificate
- Must not be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the issuer's jurisdiction

The Certification Authority / Browser Forum formally ratified the initial version of the EV SSL guidelines in June 2007, marking the successful culmination of more than two years of collaborative effort.

End-Users See Green

How does a more rigorous certificate issuance process manifest itself in a visible way to end-users? In newer web browsers, the Extended Validation SSL Server Certificates trigger the automatic display of a **green address bar**, as shown in Table 1.

Table 1: Examples of an Address Bar for a Web Site with EV SSL, and a Companion Trust Mark

Web Browser	Address Bar for a Web Site with an EV SSL Server Certificate	Trust Mark
Microsoft IE 7.0 or higher	 https://www.woodgrovebank.com Thawte Inc [US] *Internet Explorer 7+	Secured by thawte 2005-00-00

Source: Thawte, www.thawte.com/ssl/extended-validation-ssl-certificates, January 2011

Both the organization that owns the EV SSL Server Certificate (e.g., *Wood Grove Bank*) and the name of the Certification Authority that issued it (e.g., *Thawte*) are displayed, to increase end-user confidence that they are on a legitimate site. Over time, more and more end-users are becoming conditioned to "look up" to the green address bar, which gives them higher assurance that their personal data is being encrypted while in transit and that the web site they are connecting with has been authenticated based on a more rigorous industry standard. Many providers of SSL Server Certificates and EV SSL Server Certificates also offer a companion trust mark – for example the *Thawte Trusted Site Seal*, as shown in Table 1 – as a complementary visual indicator of end-user confidence.

Virtually all web browsers currently in use recognize and support EV SSL Server Certificates. In addition, for much older web browsers an optional feature known as **Server-Gated Crypto (SCG)** can be used to increase (or "step up") the strength of the encrypted session from 40-bits or 56-bits to 128- or 256-bits. This simply means that site owners can protect a higher total percentage of their end-user subscribers using the highest levels of encryption currently in use (although causing these older browsers to be upgraded, if at all possible, is arguably the better and more secure choice).

Site Owners See Green, Too

A more rigorous issuance process means that Extended Validation SSL Server Certificates are also more expensive – typically by about two- to three-times – than a traditional SSL Server Certificate. If they cost more money to buy and deploy, how does the green address bar and higher assurance translate to business benefits for the site owners?

The answer lies in increasing end-user trust in the legitimacy and security of their web site, which directly translates into the confidence to conduct more transactions online. Examples of the positive impact realized from the deployment of EV SSL Server Certificates include:

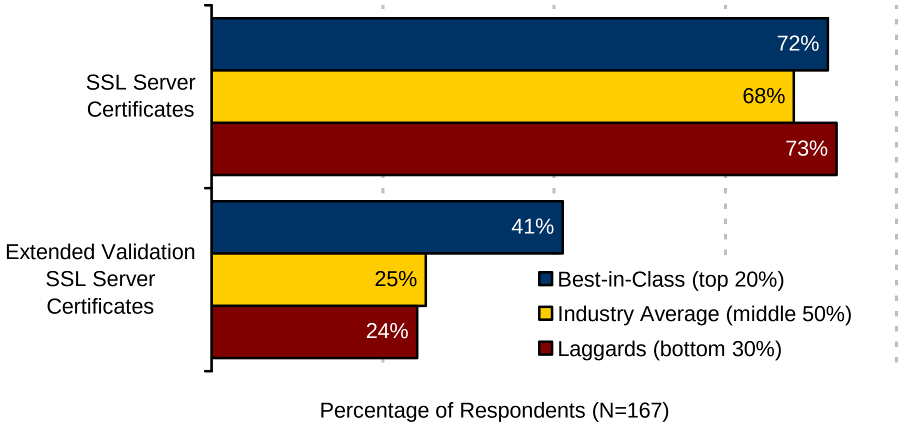
- A debt consolidation site reported an 11% increase in its online form completion rate
- A retail footwear site reported a 13% decrease in abandoned shopping carts
- An originator of home mortgages reported a 10% increase in online enrollments

Each organization must calculate the financial impact on its own online business, based on its own transaction volumes and values. Still, these examples show that EV SSL Server Certificates represent one of the most straightforward cost justifications to be made in IT Security. This helps to explain why the top-performing organizations in Aberdeen's research were 1.7-times more likely than the lagging performers to deploy EV SSL Server Certificates (Figure 2).

"The cost per lead in our business has grown to about $20 because of drastically reduced user confidence. We never dreamed that deployment of Extended Validation SSL Server Certificates would be so effective at addressing this issue."

~ President,
Debt Consolidation Service

Figure 2: Current Use of SSL, EV SSL by Maturity Class



Source: Aberdeen Group, January 2011

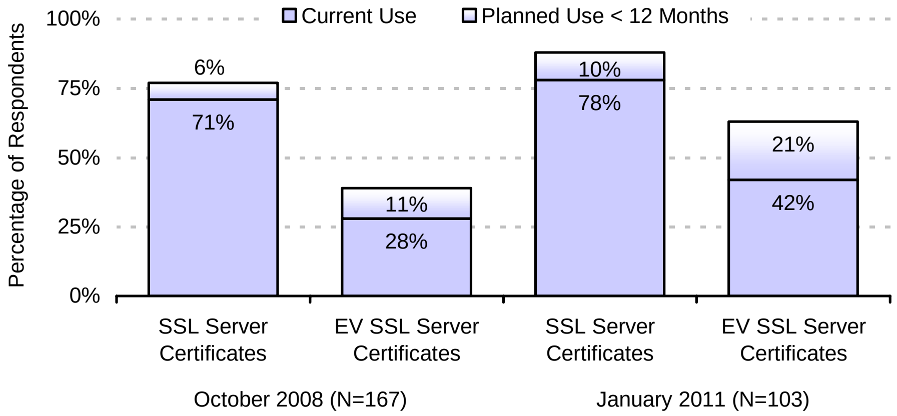
Directionally, the market trend observable in Aberdeen's benchmark data is strongly in favor of increased use of EV SSL Server Certificates (Figure 3):

- Current use of the less expensive SSL Server Certificates outstripped that of EV SSL Server Certificates by a factor of 2.5-

times in an Aberdeen study from October 2008, a gap which shrunk to a factor of 1.8-times in Aberdeen data from January 2011

- Planned deployments in the next 12 months favor EV SSL by a factor of about 2-times, and
- Current evaluations favor EV SSL by a factor of nearly 3-times.

Figure 3: Current Use, Planned Use in Next Year (all respondents)



Source: Aberdeen Group, January 2011

Solutions Landscape (illustrative)

Extended Validation SSL Server Certificates are offered by a wide range of organizations worldwide; the following provides a partial list:

- *Comodo CA Ltd*
- *DigiCert, Inc.*
- *Entrust, Inc.*
- *GeoTrust, Inc.*
- *GlobalSign*
- *GoDaddy.com, Inc.*
- *Network Solutions, LLC*
- *PGP TrustCenter*
- *QuoVadis Ltd.*
- *SwissSign AG*
- *Thawte, Inc.*
- *Trustwave*
- *VeriSign, Inc.*
- *Verizon Business*

Summary and Recommendations

Extended Validation SSL Server Certificates directly address the need to increase end-user confidence in transacting online, by providing an intuitive visual indicator: the green address bar, commonly used in combination with a companion site seal. By providing end-users with visual cues that the web site they are connecting with has been authenticated based on a more rigorous industry standard, EV SSL Server Certificates establish a higher level of assurance that they are on a legitimate web site, and that their personal data is being encrypted while in transit.

Increasing end-user trust in the legitimacy and security of the web sites they visit translates directly into end-user confidence to conduct more transactions online, and higher revenues and margins for site owners. Deployment of EV SSL Server Certificates has a straightforward cost justification for commerce-oriented web sites, and should be considered as a standard element of any organization's multi-layered approach to online security.

For more information on this or other research topics, please visit www.aberdeen.com.

Related Research	
The Case for Enterprise Key Management: Higher Complexity and Scale at Lower Cost; June 2010 *The CIO's View of Enterprise Key Management*; June 2010	*Web Security in the Cloud*; May 2010 *The Encryption Key Lifecycle*; November 2008 *Managing Encryption: The Keys to Your Success*; October 2008

Author: Derek E. Brink, Vice President and Research Fellow, IT Security (Derek.Brink@aberdeen.com)

For more than two decades, Aberdeen's research has been helping corporations worldwide become Best-in-Class. Having benchmarked the performance of more than 644,000 companies, Aberdeen is uniquely positioned to provide organizations with the facts that matter — the facts that enable companies to get ahead and drive results. That's why our research is relied on by more than 2.5 million readers in over 40 countries, 90% of the Fortune 1,000, and 93% of the Technology 500.

As a Harte-Hanks Company, Aberdeen's research provides insight and analysis to the Harte-Hanks community of local, regional, national and international marketing executives. Combined, we help our customers leverage the power of insight to deliver innovative multichannel marketing programs that drive business-changing results. For additional information, visit Aberdeen http://www.aberdeen.com or call (617) 854-5200, or to learn more about Harte-Hanks, call (800) 456-9748 or go to http://www.harte-hanks.com.