

WHITE PAPER

When It's Tax Time, EV SSL Is Essential for Online Filing

Sponsored by: Symantec

Sally Hudson
February 2011

IDC OPINION

As more and more transactions are moving to the Internet, both providers and consumers are increasingly concerned about the security of their digital environment. Advanced authentication technologies are being adopted at a greater rate than ever before, driven primarily by:

- ☒ Increased industry and government regulations for data security and privacy
- ☒ Steadily increasing online interactions in government-to-citizen, business-to-consumer, business-to-business, and employer-to-employee relationships
- ☒ Increasingly sophisticated threats from hackers, phishing, and other criminal organizations or entities

Corresponding with the rise in online criminal activity is the desire from technology consumers that security be both proactive in nature and easy to use. Extended Validation SSL (EV SSL) can help in meeting these criteria.

METHODOLOGY

IDC's industry analysts have been measuring and forecasting IT markets for more than 30 years. The actual strategy incorporates information from four different but interrelated sources:

- ☒ Reported and observed trends and financial activity in 2009 as of the end of April 2010, including reported revenue data for public companies trading on North American stock exchanges (CY 1Q04–4Q04 in nearly all cases)
- ☒ Product briefings, press releases, and other publicly available information (IDC's analysts meet with hundreds of vendors each year. These briefings provide an opportunity to review current and future product strategies, revenue, shipments, customer bases, target markets, and other key product information.)
- ☒ Vendor financial statements and related filings (Although many software vendors are privately held and choose to limit financial disclosures, information from publicly held companies provides a significant benchmark for assessing informal market estimates from private companies. IDC maintains an extensive library of financial and corporate information focused on the IT industry. We further maintain a detailed revenue-by-product-area model for more than 1,200 worldwide vendors.)

- ☒ IDC demand-side research (This includes thousands of interviews annually and provides a powerful fourth perspective for assessing competitive performance. IDC's user strategy databases offer a compelling and consistent time-series view of industry trends and developments. Direct conversations with technology buyers provide an invaluable complement to the broader survey-based results.)

IN THIS WHITE PAPER

IDC examines the role of VeriSign Authentication Services' EV SSL technology as it is used by organizations preparing online tax forms to submit to the Internal Revenue Service (IRS). VeriSign Authentication Services, acquired by Symantec in 2010, is an industry-leading vendor in its own right within the IT security space. Over the past decade, VeriSign Authentication Services has designed its Internet technologies to enable companies and consumers worldwide to conduct commerce and communicate with a high level of trust.

SITUATION OVERVIEW

The VeriSign seal is available in 13 different languages and is seen up to half a billion times by consumers every day. More than 100,000 domains in 165 countries display the VeriSign seal. It is a defensible statement that the VeriSign seal is easily the most recognized trust mark on the Internet. Symantec provides security enablement to enterprise, consumer, and government communities. Security should enhance (not prevent) business enablement, which is especially important during these tough economic times.

The Internal Revenue Service and Policy for Online Tax Filing Service Providers

In July 2007, the IRS issued an e-file rule requiring all authorized IRS e-file providers to submit to the IRS the uniform resource locator (URL) of Web sites they own or operate through which taxpayer information is collected, transmitted, processed, or stored. This requirement remains mandatory for all authorized IRS e-file providers.

As of January 1, 2010, the IRS has mandated new security, privacy, and business standards to better serve taxpayers and protect the information collected, processed, and stored by online providers of individual income tax returns. (Individual income tax returns generally refer to the 1040 family of returns.) These new standards are intended to supplement the Gramm-Leach-Bliley Act and the implementing rules and regulations promulgated by the Federal Trade Commission.

According to the IRS documentation, the security and privacy objectives of some of these standards are:

- ☒ To set minimum encryption standards for transmission of taxpayer information over the Internet and authentication of a Web site owner's and/or operator's identity beyond that offered by standard SSL Certificates

- ☒ To provide a periodic external vulnerability scan of the taxpayer data environment; protection against bulk filing of fraudulent income tax returns
- ☒ To isolate and investigate potentially compromised taxpayer information in a timely fashion

These standards also address certain business and customer service objectives such as instant access to a Web site owner's and/or operator's contact information and an online provider's written commitment to maintaining physical, electronic, and procedural safeguards of taxpayer information that comply with applicable law and federal standards.

Extended Validation SSL Certificates

The IRS-mandated standards of EV SSL use for online providers states that all online providers of individual income tax returns shall possess a valid and current EV SSL Certificate using SSL 3.0/TLS 1.0 or later and minimum 1024-bit RSA/128-bit AES.

To be in compliance with the Payment Card Industry Data Security Standard (PCI DSS), online providers of individual income tax returns are required to contract with an independent third-party vendor to run weekly external network vulnerability scans of all their "system components." All scans must be performed by a scanning vendor certified by the Payment Card Industry Security Standards Council and listed on its current list of approved scanning vendors (ASVs). In addition, online providers of individual income tax returns whose systems are hosted must ensure that their host complies with all applicable requirements of the PCI DSS.

Authentication: A Prerequisite for Online Security

Authentication is a significant technology within the identity and access management (IAM) market. IDC defines IAM as a comprehensive set of solutions used to identify users in a system (employees, customers, contractors, etc.) and control their access to resources within that system by associating user rights and restrictions with the established identity.

What are authentication services? SSL Certificates constitute a comprehensive authentication solution, including EV Certificates and related identity and authentication services. Through its SSL Certificate offerings, Symantec issues certificates to legitimate Web sites, allowing customers to have trust and confidence that sensitive information being transmitted over the Internet is both safe and secure. In addition, by confirming the legitimacy of the business through these authentication practices, consumers can also feel confident that the information sent is going to the business to which they intend it to go and not to an entity behaving fraudulently. An EV SSL Certificate is issued according to a specific set of identity verification criteria. These criteria require extensive verification of the requesting entity's identity by the certificate authority (CA) before a certificate is issued. The standard for issuing EV SSL Certificates was established by a group called the CA/Browser Forum, which consists of leading CAs as well as browser manufacturers that came together to create this standard for business and Web site authentication. Certificates issued by a CA under the EV guidelines are not structurally different from other certificates, which

is important for them to still work with legacy browsers. However, EV SSL Certificates contain an "E marker" that gives high-security Web browsers information to clearly identify a Web site's organizational identity.

When Internet users equipped with the latest versions of the leading Web browsers visit a site protected by VeriSign EV SSL Certificates, the address bar on their browser turns green. The green address bar offers immediate reassurance that users have reached a site whose authenticity has been verified by a recognized SSL CA such as Symantec — and not a fraudulent, copycat Web page created by identity thieves to steal sensitive personal data, including Social Security Numbers and credit card information.

More than 24,000 Web sites already rely on VeriSign EV SSL Certificates, including FileYourTaxes.com, an early provider of online tax filing services. FileYourTaxes.com deployed VeriSign EV SSL in 2009 to further its commitment to providing safe and trusted services using advanced, proven technology.

Since its inception in 1996, FileYourTaxes.com continues to be a leader in technology and innovation, bringing the benefits of efile to its customers, the American taxpayers. "As an initial participant of the IRS online filing pilot, we realized our business was about obtaining the Taxpayer's trust and delivering confidence in addition to developing a simple, easy-to-use solution for the consumer to directly efile their return to the IRS. The VeriSign Trust Services, specifically their seals and certificate products, promote consumer confidence. When we learned that EV Certificates would provide additional transparency to the consumer, we were excited to again be a pioneer in our industry, integrating this valuable tool within our system, providing added assurance and confidence to customers. As a result, we have seen greater consumer confidence and noted that other industry members followed suit," said Timur Taluy, CEO of FileYourTaxes.com.

"We feel confident that this integration was beneficial in responding to the demands generated by growing government regulations in strengthening security and privacy aspects of the providers," said Taluy. "Likewise, it helped mitigate certain customer barriers to more assuredly doing business online while possibly minimizing certain levels of threat types that are increasingly prevalent in the Web."

FUTURE OUTLOOK

Scenarios

The IRS states that compliance with these standards is mandatory, effective as of January 1, 2010.

IDC forecasts that the adoption of advanced authentication technology will almost double in the next four years as businesses, governments, and social networks strive to implement safe, private, and secure ways to interact with the public. License and maintenance revenues for advanced authentication, which is a subsegment of the overall IAM market, accounted for \$520 million worldwide in 2009 and are predicted to reach \$892 million by 2014.

CHALLENGES/OPPORTUNITIES

For VeriSign, and perhaps the online U.S. tax filing community as a whole, the greatest challenge lies in the public's perception of fundamental flaws in online computer security mechanisms. This is especially true in sensitive areas such as tax preparation and filing, banking, and financial services. While great strides have been made in these areas, and as more citizens file their taxes via online services each year, security breaches are still occurring and are widely publicized, which in turn makes the general public more cautious when using electronic filing methods.

The primary opportunity revolves around the trust associated with the VeriSign brand combined with increased levels of security to meet government mandates. The software presents no implementation or maintenance contingencies for subscribers, which adds to the overall appeal.

CONCLUSION

Increasing regulatory compliance mandates in the United States (and internationally) and continually evolving ID theft and fraud techniques will continue to drive organizations to look for better ways to cost-effectively manage their security infrastructure. Within an online transaction setting, EV SSL can serve as a strong first line of defense. The rising tide of ID fraud, ID theft, and privacy violations is shaping the way we look at Internet security today. The news media regularly reports on online crime and its impact on individuals, businesses, and even national security. These issues will continue to drive legislation for stricter security and policy enforcements. Security and regulatory requirements will increase, not decrease, going forward, and companies that can provide nonintrusive, highly reliable, and proven security solutions are positioned to do well over the next several years.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2011 IDC. Reproduction without written permission is completely forbidden.