The Questions that I am Most Frequently Asked by New Buyers of SSL Certificates

FROST & SULLIVAN

Frost & Sullivan White Paper

Chris Kissel, Industry Analyst

THE QUESTIONS THAT I AM MOST FREQUENTLY ASKED BY NEW BUYERS OF SSL CERTIFICATES

CHRIS KISSEL, INDUSTRY ANALYST | FROST & SULLIVAN

Very few people have their work lives dominated by managing Secure Sockets Layer (SSL) certificates. At the end of the day, people want to make sure their Web properties are secured with as little friction as possible; SSL certificates are a means of accomplishing that goal. As a result, new buyers are constantly entering the market as people launch new Web properties.

Symantec requested that I put together the most commonly asked questions that I encounter to help those new SSL certificate buyers, especially those that are considering Symantec as their vendor of choice. If you are new to the SSL certificate market, I am sure that you will have at least one of these questions as well.

Q. Why do I need to secure my website with an SSL certificate?

A. Without some type of encryption technology, data sent from Web servers/sites to end users would be vulnerable to intercept or man-in-the-middle attacks. Web servers and Web browsers rely on the SSL protocol to help users protect their data during transfer by creating a uniquely encrypted channel for private communications over the public Internet. Each SSL certificate consists of a key pair as well as verified identification information. A "SSL handshake" between the Web browser (or client) and Web host/server completes a unique session key.[1]

Q. Why should I buy from Symantec?

A. The selection of an SSL certificate vendor revolves around three primary considerations: quality, performance and ownership experience. "Why Symantec" is best answered using these criteria.

Symantec solutions protect information for people, successful enterprises, global industries, and beyond. Symantec is uniquely positioned to address the complex and rapidly evolving needs of sophisticated customers across security and information management, irrespective of device or platform. Symantec offers the high-quality SSL/TLS (Transport Layer Security) certificates, the robust and secure Web infrastructure, and global resources for tech support.

Performance is another important feature when considering SSL/TLS certificates. Symantec rootkeys will have the greatest browsers and server support. The time to load Web pages is partly contingent on the time for the key-authentication process. Symantec invests to maximize certificate performance; as an example, Symantec has the fastest OCSP average response time (September 2014, Dynatrace). In addition, Symantec has a proprietary architecture to facilitate all aspects of SSL certificate performance.

Finally, the ownership experience must enable frictionless certificate deployment. SSL certificate ownership can be thought of as a continuous lifecycle. At the time of purchase, the Symantec Assistant makes it easy for customers to install and activate SSL certificates. Advanced SSL tools are standard with all SSL/TLS certificate purchases. Symantec creates advantages for its customers in all aspects of SSL ownership, including fast certificate revocation, breach detection, on-going tech support, and account management.

[1] For more information, please see SSL by Symantec - Learn How SSL Works | Symantec

Tech support is a major differentiator for customers choosing a CA. A customer can access the Symantec technical support 24/7 every day of the year. Symantec offers customer support in more than 150 countries. Different data centers support as many as five languages and, in total, global tech supports more than 20 languages.

Q. Why do we need to upgrade from secure hash algorithm (SHA-1)?

A. The SSL certificate ecosystem is requiring the forced deprecation of SHA-1 certificates over concerns that the computational power needed to break the encryption is becoming available. In 2010, the US National Institute of Standards and Technology (NIST) started transitioning applications away from SHA-1. In 2013, Microsoft announced its deprecation policy on SHA-1, meaning Windows will stop accepting SHA-1 certificates in SSL by January 1, 2017. Currently, Google includes Web security as a criterion in its Web search, and SHA-1 certificates will likely be rated lower than SHA-2, elliptic curve cryptography (ECC), or Transport Layer Security (TLS) certificates.

Q. The PCI-DSS recently said that currently no encryption standard is safe. What will Symantec do if encryption standards are changed?

A. Symantec works exhaustively with the CA/Browser Forum to establish global standards for the encryption process, the deployment, and validation of SSL certificates. However, Symantec is also instrumental in working with leading industry consortia (NIST, Sarbanes-Oxney, HIPAA, etc.) toward developing the types of certificates that meet with the unique security concerns of vertical markets.

Q. What will Symantec do if encryption standards change during my licensing contract obligation?

A. Symantec hopes to address those types of concerns before they arise. Unfortunately, the wholesale substitution of PKI keys is not without precedence. In April 2014, the Heartbleed Bug was a type of exploitation that targeted servers running OpenSSL protocols. Roughly 18% of the world's servers were at risk. The only way that customers could be certain that their Web services were not vulnerable was to revoke all existing SSL certificates and replace them with new certificates. Symantec supplied this service at no additional cost.

Q. If I go shopping, I find that Symantec Extended Validation (EV) certificates are more expensive than most; why is this so?

A. Symantec SSL/TLS certificates are among the most expensive EV certificates, but also provide the most value. The formal PKI encryption is only a small part of what SSL certificates provide.

With close to a billion impressions per day, the Norton Secured Seal is an indispensable tool and is valued by business customers for its proven ability to provide consumers a secure online experience while instilling confidence and trust in their website (Fran Roche, 2012).

By displaying the Norton Secured Seal on a website, businesses can attract new visitors while maintaining high levels of traffic that are crucial to a website's success. The seal can also help reassure these visitors that they can trust the link, trust the site, and trust the transaction with the seal present at all stages of the purchase process (Fran Roche, 2012).

Symantec offers a complete Web environment in support of SSL certificates. Websites are frequently scanned for malware—the importance of this cannot be understated for customers that offer services dealing with financial records or personally identifiable information (PII). Diminishing the possibility of phishing attacks emanating from Web sites is a requisite for a company's reputation.

Symantec additionally offers certificate algorithm agility. The Symantec ECC 256-bit certificate has a compact but effective algorithm. The encryption is as powerful as a 3072-bit RSA certificate. However, because the encryption has a low footprint, it consumes a small profile on the server. Premium or Symantec Secure Site Pro SSL Certificates can be issued with any of three different encryption algorithms: ECC, RSA, or DSA (Digital Signature Algorithm). In fact, RSA and DSA encryption algorithms can be supported simultaneously on the same SSL certificate.

Lastly, some customers may need technical support. Symantec has the most resources globally to help customers with support issues. Symantec offers customer support in more than 150 countries and in more than 20 languages.

Q. The SSL/TLS certificate is a transparent event to the end user. After a secure connection is made, is there anything else in the experience for the user?

A. The secure connection is seamless to the end user, but not necessarily transparent to the end user. For consumers, trust comes in the form of a secure transaction. The https:// browser prefix indicates a secure link transaction. When a customer enters a site protected by an EV certificate, the browser field turns green.

Norton™ SECURED

Visitors to websites like assurances. The Norton Secure Seal has been shown to inspire consumer confidence. In an international online consumer study, 90% of respondents are likely to continue an online purchase when they view the Norton Secured Seal during the checkout process. In North America, the Norton Secured Seal guards 81% of the Top 500 eCommerce sites.

Q. Still, a certificate is just a certificate; once installed, does the certificate have additional value?

A. On August 8, 2014, Google invoked "secure website" as a factor in ranking. A site that has an "Always on SSL" improves its placing in the Google Search engine.

How you protect your network is up to you (and Symantec can help you do that). However, as a part of the SSL certificate purchase, Symantec periodically scans its certificates for cross-site scripting (XSS) or SQL injection (SQLi) vulnerabilities. Symantec also offers website vulnerability assessments and daily website malware scans; Symantec customers minimize the risks of propagating viruses or getting blacklisted by search engines. In its long history of selling SSL/TLS certificates, Symantec has never suffered a major breach.

Q. What is a certificate signing request (CSR) and how do I generate it?

A. Before an SSL certificate is purchased, a site administrator will need to generate a Certificate Signing Request (CSR) for the server on which the certificate will be installed.

A CSR is used by a certificate applicant to send encrypted information to the CA. The CA in turn verifies and includes information such as the fully qualified name of the domain, the legal business name, the department name (HR or IT for example), the business address, and country. The insertion of a digital signature from the CSR requester prevents other entities from using the public key.

As a part of an EV SSL certificate purchase from Symantec, the SSL Assistant tool is included. The SSL Assistant will generate the SSL certificate for you.

Q. How can I determine if my SSL/TLS certificates are installed correctly?

A. One of the reasons to work with Symantec is to leverage the expertise of the company behind the certificate. Through Symantec SSL Assistant, customers can use several setup wizards for SSL certificate self-installations. Symantec Encryption Management Server Setup Assistant, Windows boot server assistant, shared clustered set up, and setup.exe double-click icon are examples of wizards used by customers for configurations. The Installation Checker is a part of the SSL Toolkit.

Auckland
Bahrain
Bangkok
Beijing
Bengaluru
Buenos Aires
Cape Town
Chennai
Dammam
Delhi
Detroit
Dubai
Frankfurt
Herzliya
Houston
Irvine
Iskander Malaysia/Johor Bahru
Istanbul
Jakarta
Kolkata
Kotte Colombo
Kuala Lumpur
London
Manhattan
Miami
Milan
Moscow
Mountain View
Mumbai
Oxford
Paris
Pune
Rockville Centre
San Antonio
São Paulo
Seoul
Shanghai
Shenzhen
Singapore
Sydney
Taipei
Tokyo
Toronto
Valbonne
Warsaw

Silicon Valley
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10,
Suite 400
San Antonio, TX 78229
Tel 210.348.1000
Fax 210.348.1003

London
4 Grosvenor Gardens
London SWIW 0DH
Tel +44 (0)20 7343 8383
Fax +44 (0)20 7730 3343

877.GoFrost
myfrost@frost.com
www.frost.com

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?

For information regarding permission, write:
Frost & Sullivan
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041