FROST & SULLIVAN

Symantec: Using Always-on SSL/TLS to Maximize Web Security and Enhance the End-user Experience

Best practice ensures better opportunities for business presence in search results

A Frost & Sullivan White Paper

INTRODUCTION: ALWAYS-ON SSL/TLS

As great as the Internet is for adding depths to business applications and enriching relationships through social media, a trade-off exists—intellectual property and personally identifiable information (PII), such as debit and credit cards, are potentially exposed. Adding depth and function to Web applications and websites also increases the opportunity for cyberattacks and makes websites and end users more vulnerable.

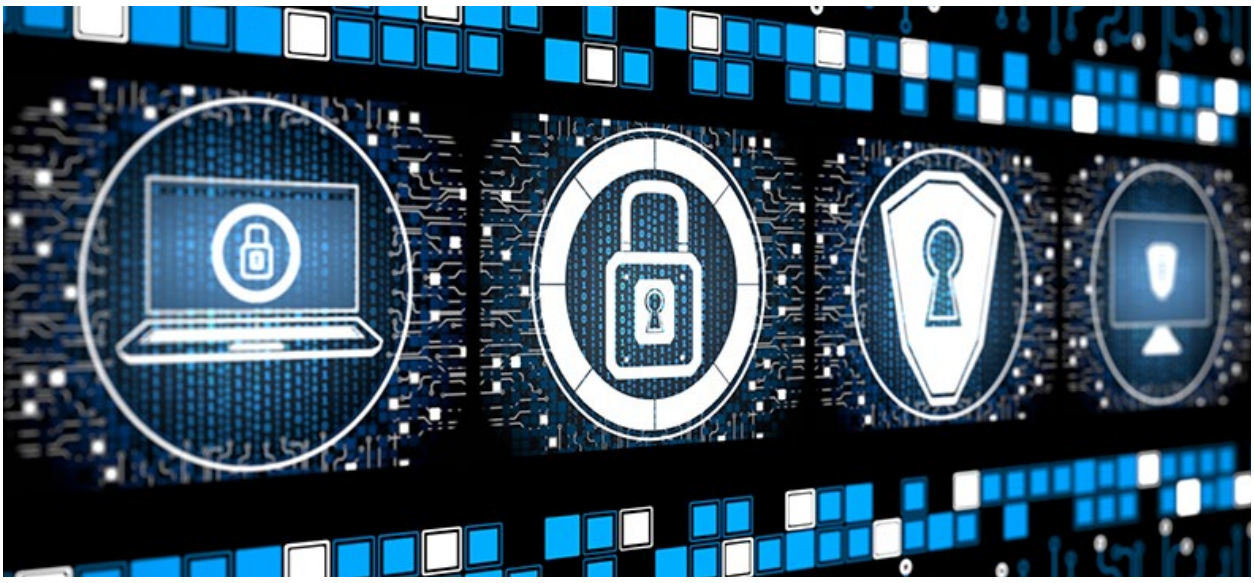
Encryption is increasingly being adopted as Web properties look to improve security, https:// or data-in-transit. Hypertext Transfer Protocol Secure (HTTPS)-enabled websites ensure privacy of the bi-directional communications between websites and their visitors through the Internet by encrypting the communications. While these communications could conceivably be intercepted by a third party, they are difficult to decipher without the proper decryption keys. Certificate Authorities (CA) issue SSL/TLS certificates, which include public keys, identity information, and other data.

> *"SHA-1 SSL certificates are being deprecated in large part because the computing power needed to replicate the unique algorithms in the PKI handshake is becoming possible using commercial off-the-shelf computing devices."*

ALWAYS-ON SSL/TLS

Always-on SSL/TLS is a best practice advocated by Internet consortia, which includes members of the CA Security Council, the CA/Browser Forum, and the Online Trust Alliance. The major CAs, including Symantec, advocate the use of Always-on SSL/TLS. The combination of Always-on SSL/TLS and SSL/TLS products and services from providers like Symantec enables top-of-the-line Web security, protects and promotes a company's business presence, and gives a Web visitor a secure session experience.

Always-on SSL/TLS is not just a set of discrete best practices; Always-on SSL/TLS is an integrated Web security posture. The table below summarizes the differences between the state of a website before Always-on SSL/TLS use and what happens when Always-on SSL/TLS is implemented.[1]



1 There are several good publicly available sources that explain more technical aspects of Always-on SSL/TLS, including documents from the Online Trust Alliance website and Always-on SSL | Symantec.

Figure 1: Before Always-On SSL/TLS and After Always on SSL/TLS

Before Always-on SSL/TLS	After Always-on SSL/TLS
A web session might not be protected end to end. Often companies with a Web presence only protect the title page of the website. When a Web visitor navigates from page to page within the Web session, the end user's cookies are exposed, and various Web pages may not be properly secured.	**Always-On SSL/TLS is a table stake in website security.** The title page is encrypted, and all transitions to different pages within a website are secured (including cookies).
Mixed content is a concern. The problem is most acute in social networks where third parties share links to websites and files. If the content is linked to an HTTP link, an attacker could create an exploit through a previously secured channel.	**Invoking HTTP Strict Transport Security (HSTS).** The protocol enables Web visitors to interact with websites only through encrypted communications.
A diminished ranking in the Google search engine. The Google search engine used to work largely on an algorithm based on keyword(s) relevancy.	**Higher rankings in the Google search engine.** As of August 6, 2014, Google announced that the security of a website would become part of the matrix determining keyword rankings.
The man-in-the-middle attack (MITM) becomes a serious adversary. The MITM can use a packet sniffer like Firesheep to obtain information from cookies. Additionally, MITM can spoof an end-user's credentials without any hint of detection from the end user or the Web application browser.	**Minimize the risks of a MITM attack.** The initial site request is encrypted. When an end user attempts to access different parts of a website, they are sent to an encrypted channel (encrypted in transit, decrypted upon arrival).
Weak security posture. Web visitors are less confident that their interactions on the site are secure and as a result may minimize their Web visits.	**Always-On SSL/TLS builds trust between vendors and clients.** Social media sites Facebook and Twitter practice Always-On SSL. In fact, Twitter won the 2014 Online Trust Alliance award as the most trustworthy website because of its use of perfect forward secrecy and Always-On SSL. For companies like PayPal or eBay that continuously conduct cash transactions online, a breach would severely hamper operations.

Source: Frost & Sullivan

HTTPS protection is needed beyond the title page. Most Web visitors will access a site via the title page (www.company.com). However, when a visitor wants to navigate from the title page to the payment page or any other page, that process needs to be secured.

Websites often use cookies to store information such as usernames, passwords, addresses, or session data. Without the protection provided by HTTPS, a man-in-the-middle attack (MITM) may be able to "sidejack" the cookie. A sidejack occurs when a MITM intercepts information from the cookie, including PII or passwords that can be used to impersonate the activities of the authentic end user. The MITM usually goes undetected by a website's Web server.

SELECTING THE PROPER CERTIFICATE AUTHORITY (CA) IS ESPECIALLY IMPORTANT WHEN IMPLEMENTING ALWAYS-ON SSL/TLS

The traditional role of the CA has been to issue and help clients install SSL/TLS certificates. Increasingly, however, the CA is being called on to help Web administrators manage the entire SSL/TLS certificate lifecycle. From certificate monitoring to certificate signing request (CSR) generation, SSL/TLS certificate management tools from a CA can help administrators implement and maintain Always-On SSL/TLS.

A CA's role extends beyond issuing SSL/TLS certificates. One of the criteria for Google keyword search is website security. If a browser service provider finds evidence of malware on a website, the site can be blacklisted—the end user gets a warning that reads, "This site may harm your computer." While this warning is intended to prevent malicious websites from masquerading as legitimate businesses, it also means that legitimate businesses with malware on their sites will be blacklisted as well. Symantec offers both malware and website vulnerability scanning for common vulnerabilities such as cross-site scripting (XSS) and SQL injection (SQLi).

The types of SSL/TLS certificates offered by CAs are important both in terms of security and performance. The current requisite for Payment Card Industry Data Security Standard (PCI-DSS 3.0) and several other industries is a minimum 2048-bit RSA encryption. Companies looking for added security may consider Elliptic Curve Cryptography (ECC) certificates to implement Perfect Forward Secrecy (PFS), a protocol that helps prevent historical data from being decrypted. A Symantec 256-bit ECC certificate offers the equivalent security of a 3072-bit RSA certificate and is roughly 64,000 times harder to break than a RSA 2048-bit encrypted SSL/TLS certificate. In addition, ECC certificates provide strong performance for mobile applications.

Online Certificate Status Protocol (OCSP) is the request/response mechanism used for SSL/TLS certificate revocation checks. A quick response time contributes to an optimal Web user experience.

When a browser, application or device encounters a certificate that it does not recognize as issued from a trusted entity, a warning message is triggered or communication is terminated. As such, a CA that is widely accepted as a trusted entity across a wide range of platforms increases the ease of doing business for an organization. Symantec, as the first commercial CA, has wide ubiquity for its SSL/TLS certificates. From operating systems to browsers to devices, including mobile set-top boxes and ATMs, Symantec SSL/TLS certificates are well supported—more than other CAs.

SSL certificates are giving way to Transport Layer Security (TLS) certificates. Like SSL certificates, TLS certificates are a type of X.509 certificate. Unlike SSL certificates, TLS certificates use a dedicated transport layer that provides a complete cryptographic security layer for confidential information transmitting between servers. Many companies use TLS 1.1 and TLS 1.2 certificates to establish secure communications between internal servers. Symantec TLS certificates are supported by all major browsers.

Figure 2: Choosing Symantec SSL/TLS Certificates for Security and Performance

Source: Frost & Sullivan

ALWAYS-ON SSL/TLS MEANS MORE THAN JUST CERTIFICATES

The transition to Always-on SSL/TLS represents a change in the relationship between businesses and the CA vendors. The SSL/TLS certificate is an important part of Internet security; however, CAs are now expected to help with all aspects of the SSL/TLS certificate process, including acquisition, installation, and continued management of certificates. Here is how Symantec differentiates itself from other SSL/TLS certificate vendors:

- **A decade of SSL/TLS certificate leadership.** Frost & Sullivan has tracked the global SSL/TLS certificate market since 2008. Symantec has been the market leader and continues its dominance; in 2015, Frost & Sullivan estimates Symantec earned a 54% share of the $1.1 billion SSL/TLS market. Symantec has forged relationships with IT administrators and in many cases is a trusted advisor to customers in selecting the right SSL/TLS certificates for their server configurations.
- **Premium Certificates. Symantec SSL/TLS certificates have never suffered a major security breach.** To back its certificates, Symantec has the highest warranty in the industry; EV certificates carry a $1.75 million indemnity for certificate holders against certain losses resulting from a breach. The Symantec SSL Installation Checker allows customers to check that their SSL/TLS certificates are installed properly.
- **Exceptional customer support.** Symantec offers customer support in more than 150 countries and in more than 20 languages.

THE FINAL WORD

Businesses are looking for CAs that do more than supply SSL/TLS certificates. Companies recognize that a Web session may be the first (and only) impression that a business or customer makes with that company. Web security is important in that if a browser service provider understands or is under the impression that malware is on a website, it will blacklist the website, and a secure website is now a criterion in the Google keyword search metric. In addition, managing SSL/TLS certificates can be challenging and companies are looking for easy-to-use tools to help them simplify the life-cycle management of digital certificates.

In terms of providing Internet services, Symantec emerges as more than a SSL/TLS certificate provider; Symantec has sustaining strength as a strategic Internet security partner.

FROST & SULLIVAN

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 SW1W 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?