Six Golden Rules for Selecting an SSL or TLS Certificate

FROST & SULLIVAN

A Frost & Sullivan White Paper

OVERVIEW

The Internet was created with the best human aspirations in mind. From its nascent and humble beginnings, the intention of the Internet was to create point-to-point communications linking people and machines at light speed. The value of knowledge increases when shared.

However, as it is with well-intentioned human aspirations, the darker aspirations soon follow. Communications do not get a free pass. Thieves steal data if left unchecked. Business competitors infiltrate websites and alter files or disrupt services if left unprotected. In the 21st century, perhaps before, nation-states initiated advanced persistent threat, distributed denial-of-service (DDoS) and other cyber-attacks with the intention of crippling or destroying services.

Therefore, the fruition of the Internet cannot exist without trusted point-to-point communications. The foundation of trusted Internet communications are Secure Socket Link (SSL) certificates, an encryption technology installed on Web servers that permits transmission of sensitive data through an encrypted connection. Using a public-key infrastructure (PKI), SSL certificates authenticate the end-use website and the endpoint server, making it difficult for those sites to be imitated or forged. SSL certificates are purchased from companies known as certificate authorities (CAs).

> At the end of the day, people want to make sure their websites are secured with as little friction as possible.

The SSL certificate though is simply the tool that enables people and businesses to explore the power of the Internet. The following are use cases where SSL certificates are used to enhance business practices:

- A shop owner is having success and wants to expand his business to sell goods online.
- A major healthcare provider needs to handle sensitive personally identifiable information (PII).
- A large company needs SSL certificates to ensure encryption for internal emails.
- An online flower shop wants to purchase a strong SSL certificate because it learned that strength of the encryption code protecting a website is now a factor in the Google webpage ranking.
- A multi-national organization wants to protect its servers from unwanted intrusion and purchases SSL certificates to secure server-to-server communications.
- A financial institution wants the best protection possible for its site. The institution purchases an Extended Validation (EV) certificate because the EV certificate is the most stringent verification process in SSL certificate issuance. A customer visiting an EV-protected website can be assured that they are not visiting a phishing site.

In today's cyber environment, the SSL certificate is a necessity for any interest that wants to have a serious Internet presence, but the end-user experience has to be considered. The majority of SSL certificate purchasers have limited resources in terms of time and little experience in the proper implementation of SSL certificates. Enabling Web properties for SSL certificates is not a primary goal, but is often on the critical path to getting something done. Additionally, management of an SSL certification has to be easy throughout the entire life cycle of a certificate as organizations frequently face a dilemma refreshing SSL certificates at the time of expiry. At the end of the day, websites have to be secured with as little friction created for organizations as possible.

The SSL certificate is much more than a server-PKI key exchange. Acknowledging that there are many different use cases, these are six Golden Rules to consider when purchasing a SSL certificate:

1. **The quality of the encryption matters.** Every vertical industry requires SSL certificates that use, at a minimum, 2048-bit encryption keys. The threat landscape is becoming more aggressive; however, CAs can provide enhanced security for their customers by offering SSL certificates with stronger encryptions. An elliptic curve cryptography (ECC) 256-bit is a stronger cryptography than a RSA 2048-bit key length, but about the same as a RSA 3072-bit key. By using the ECC, customers can leverage the same supporting structure longer, even if the need for stronger security increases.

2. **CAs need to help customers get started and stay secure.** Several steps are required to make SSL certificates functional. The website administrator needs to generate a Certificate Signing Request (CSR) for the server where the certificate will be installed. The domain needs to be validated, and finally, the certificate is then installed.

   The responsibility of the CA does not end at installation. The customer needs to make sure the encryption is in compliance with industry standards as well as with the company's policy. The CA should be able to provide tools to help customers do this. For any site manager, handling a few certificates may be relatively easy to do, but handling multiple SSL certificates for different locations becomes difficult.

3. **Robust management of SSL certificates and integration of certificates into a company's IT systems prevents future business interruptions.** SSL certificate management and inventory tools should be included with any SSL certificate purchase. An IT administrator will want to have multiple roles and asset settings. Additionally, since the SSL certificate management is offline from a company's standard IT workflow, SSL certificate management should be integrated into a company's ticketing system. As difficult as it can be to configure SSL certificates for externally facing websites, often port configurations and certificates attached over multiple servers in an internal network are more problematic.

4. **The total user experience must be easy and effective.** SSL certificates are not issued in a vacuum. The leading CAs will have ubiquitous browser support, and SSL certificates will be compatible with multiple server OS. The Online Certificate Status Protocol (OCSP) is the request/response mechanism used for SSL certificate revocation checks. CAs with fast load times can accelerate response times to users' inquiries; the best CAs have the fastest load times. Additionally, PKI roots are used for internal emails and as encryption for mobile.

5. **SSL certificate issuance is an integral part of the network infrastructure.** The renewal process for SSL certificates should be automated. In some server systems, such as Microsoft Windows servers and Apache Tomcat, a new CSR has to be generated. Automated renewals help customers through the process.

Preferably the CA that issues SSL certificates has a global footprint. CAs need to have partnerships with global datacenters. Part of the investment CAs make is with datacenters globally. The CA would perform a real service for its customers if they would regularly scan their SSL certificates for cross-site scripting (XSS) or SQL injection (SQLi) vulnerabilities.

6. **The trustworthiness of the CA extends beyond the issuance of SSL certificates.** With each certificate purchase, the often overlooked value of a CA increases in importance. Customers may need the help of tech support. The reputation of the CA permeates every aspect of the SSL certificate lifecycle, including installation, fast certificate revocation, breach detection, on-going tech support, and account management. For businesses working with a CA, the best CAs instill trust when protecting cyber properties.

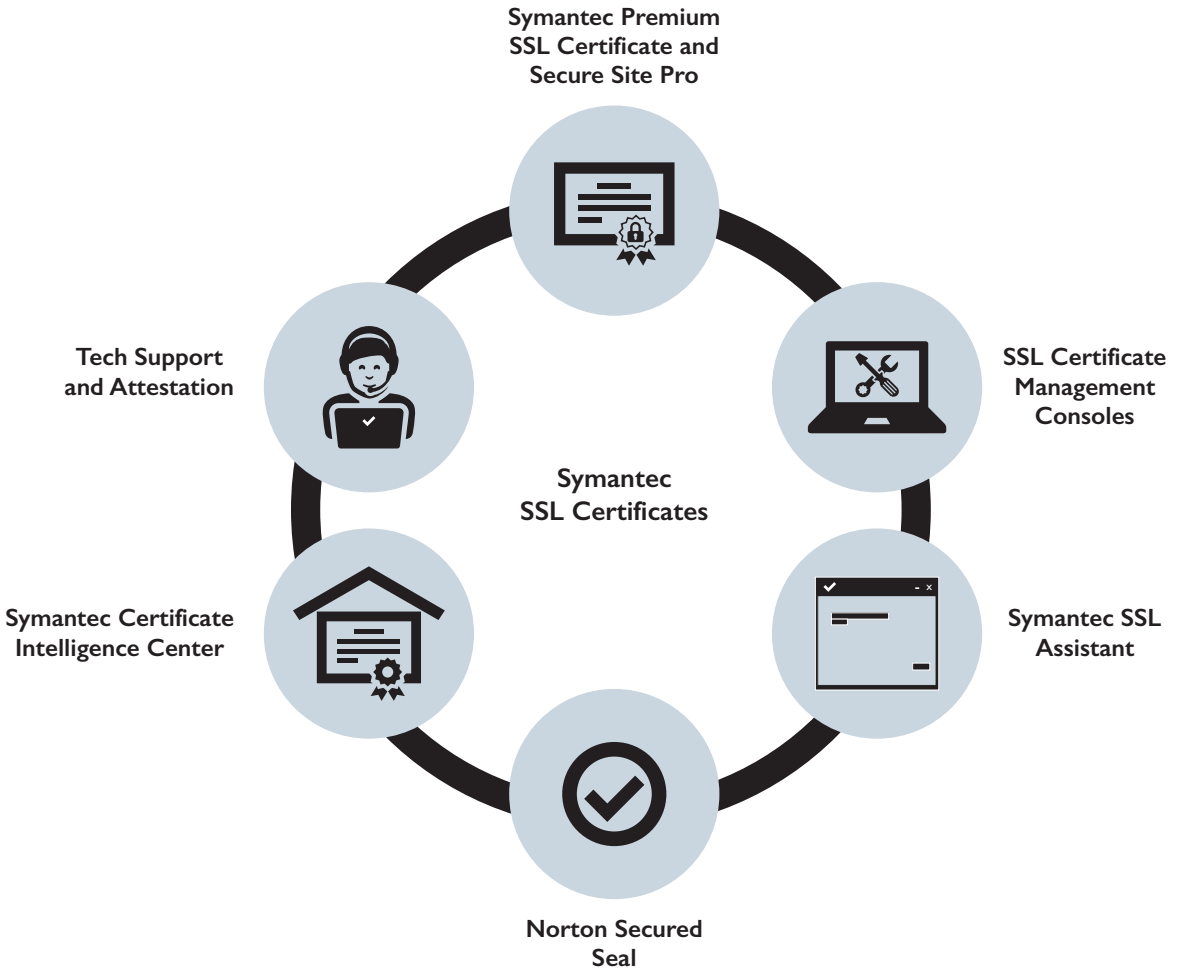
   For consumers, trust comes in the form of a secure transaction. The https:// browser prefix indicates a secure link transaction. When a customer enters a site protected by an EV certificate, the browser field turns green. In addition to these secure-site consumer protections, other companies have certificate assurance procedures also visible to visitors of a website.

The six Golden Rules are paramount in purchasing a SSL certificate and choosing a CA provider. Frost & Sullivan believes that a SSL certificate is a small part of a larger commitment.

SYMANTEC SSL CERTIFICATE ECOSYSTEM

Symantec is the global leader in SSL certificate issuance.[1] Symantec has a 58% share of a global SSL certificate market that was worth roughly $1.04 billion in 2014. Symantec is a strong service provider on both the quality of the SSL certificates that it issues, as well as in the investments Symantec makes toward offering a better SSL certificate ownership experience.

Figure 1. Symantec SSL Certificate Ecosystem



Source: Symantec, Frost & Sullivan

SYMANTEC SSL CERTIFICATES

The centerpiece of an SSL ecosystem is the certificate. Symantec differentiates in several important ways:

- **Symantec certificates have nearly ubiquitous support in the network and Internet infrastructure.** Symantec has a global reach. Symantec SSL certificates are compatible with every major browser and with almost every server OS. While SSL certificates are mostly used to protect public-facing Web sites, there are several types of server certificates used to protect other parts of the network infrastructure. TLS (Transport Layer Security) certificates evolved from SSL certificates but have important differences. 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 TLS1.1 and TLS 1.2 certificates to establish secure communications between internal servers. Symantec TLS certificates are supported by all major browsers. Along with Web sites, Symantec certificates are supported in set top boxes and ATMs—more commonly than any other CA. Additionally; Symantec uses retired PKI algorithms for certificates in heterogeneous networks and for different types of devices. Symantec certificates are used in mobile.

- **SSL certificates are protected by the largest and most secure global infrastructure.** Symantec has never suffered a security breach related to their SSL certificates due to its investments in a military-grade infrastructure, strict rigor and tightly-controlled processes. As the global leader, Symantec has relationships with leading content delivery network (CDN) service providers. Having a global footprint means Symantec SSL certificates are supported in the most datacenters.

- Symantec has a proprietary architecture to facilitate all aspects of SSL certificate performance. When combining external relationships with internal engineering, a positive cascading effect occurs. Symantec SSL certificates achieve the fastest OCSP average response times (source: September 2014, Dynatrace).

- Symantec makes superior quality SSL certificates. 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. This shortens authentication cycles. Symantec maintains the strictest validation processes in OV and EV certifications. Despite the extensive validation process, wildcard and subject alternative name (SAN) certificates can be purchased on a single certificate.

SYMANTEC PREMIUM SSL CERTIFICATES AND SECURE SITE PRO

The CA/Browser Forum establishes industry standards for the issuance of SSL certificates. The criteria for EV certificates are the most stringent. Requisites for issuing an EV certificate include verification of an organization's registered legal name, registration number, registered address, physical business address, and any assumed business names. Symantec offers further protections.

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. Premium or Symantec Secure Site Pro SSL Certificates can be issued with any of three different encryption algorithms: ECC, RSA , and DSA (Digital Signature Algorithm). In fact, RSA[2] and DSA encryption algorithms can be supported simultaneously on the same SSL certificate.

Premium or Symantec Secure Site Pro SSL Certificates offer the best EV certificate protection in the field. Symantec has an SSL Installation Checker that allows users to check if their certificates are properly installed. As Symantec offers Website vulnerability assessments and daily website malware scans, Symantec customers minimize the risks of propagating viruses or getting blacklisted by search engines.

Of course, businesses are only the constellation of clients, and Symantec offers protection for people visiting Symantec-protected Websites. The Norton Secured Seal is a recognized "seal-of-trust". A left-click on the Norton Secured Seal shows the site name, the SSL certificate status, and the proper company/organization name. The seal also shows the data transmission is encrypted and the Web site and owner are verified. More about the importance of the Norton Secured Seal will be discussed later in the whitepaper.

SSL CERTIFICATE MANAGEMENT CONSOLES: MANAGED PKI AND SYMANTEC TRUST CENTER FOR ENTERPRISE

Symantec SSL certificate management consoles are cloud-based. A key advantage to cloud-based applications is that expansion is modular and requires no new software or infrastructure equipment purchases by the client. A secure cloud application offers redundancy and full-disaster recovery. Symantec cloud infrastructure has earned the WebTrust and SOC2 certification.

Symantec Managed PKI for SSL Certificate Accounts

Symantec management tools and customer support help clients with optimizing the management of their SSL certificates on Web servers and load balancers. Also, Symantec offers a secure infrastructure for companies with a need for private certificates. These private certificates can be chained to a private root hierarchy, and managed in the same console as public facing SSL certificates.

The Symantec Managed PKI Service automates and centralizes the administration of SSL certificates. To install an SSL certificate a site administrator needs to configure: authentication, encryption, and CSR across platforms and browsers. With Symantec managed PKI, the processes are automated. The infrastructure side including the user's browser, VPN client, mail client, or other application, needs to be configured; again, the configuration processes are automated.

For enterprise-level accounts, the Managed PKI Service can be integrated with a corporate directory to populate certificate meta-data, select and enforce certificate and application policies, and publish issued certificates. PKI Enterprise Gateway functions as a local registration authority integrating with hardware security modules to protect key material.

Symantec Trust Center Account for Enterprise

The Symantec Trust Center Account for Enterprise is offered as a cloud-based service and application is complementary with the purchase of Symantec SSL certificates. Management, reporting, and audit for the full range of Symantec SSL certificates including EV, OV, SAN, and Wildcard certificates is initiated through the console.

The SSL Certificate Management Consoles combine and automate Symantec SSL certificate issuance, Web site and infrastructure configuration, certificate management, and Web site security on a single, unified platform.

SYMANTEC SSL ASSISTANT

Symantec offers several set up 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.

Norton Shopping Guarantee

Symantec offers a unique value-added service for both merchants and customers of the merchant. The Norton Shopping Guarantee is a customer-assurance program offered by ecommerce merchants to their customers for online purchases.

Symantec inserts a Norton Shopping Guarantee seal on its website as a customer accesses the site.

The program includes the following shopper protections:

For 30 days, Symantec provides consumer protection; $10,000 against ID theft.

A $1,000 purchase guarantee ensures the delivered product will be authentic and delivered on time.

A $100 price protection is included in the service. If a merchant lowers its price within 30 days of purchase, the Norton Shopping Guarantee refunds the difference in price.

With high assurance and an improved customer experience, customers are less likely to abandon their shopping cart, cancel or ask for a refund. Symantec reports the program is beneficial to both merchants and customers. Merchants are seeing, on average, a 6% increase in conversions, a 10% increase in repeat buyers, and 20% increase in profits.

NORTON SECURED SEAL

Beyond industry conventions for EV certificates, Symantec also provides the Norton secured Seal mark for Symantec SSL customers. The Norton Secured Seal is recognized as providing the "best sense of trust" according to a survey conducted by Baymard.com. The Norton Secured Seal inspires confidence from online buyers. 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, more than any other seal or no seal displayed. Over 40 million desktops worldwide using Norton Safe Web view the Norton Secured Seal next to trusted website links in search results.

Vendors have long understood the power of the Norton Secured Seal. Of the 100 largest financial institutions, 94 are secured by Symantec SSL certificates. In North America, the Norton Secured Seal guards 81% of the Top 500 ecommerce sites. In total, the Norton Secured Seal is used nearly a billion times a day in over 170 countries.

Both Web site visitors and vendors benefit from the existing Symantec best practices in SSL certificates. Sites with the Norton Secured Seal are scanned for malware daily and have vulnerability assessment testing. As a companion tool to Norton Secured Seal, Symantec offers Seal-in-Search to help ecommerce businesses drive traffic to their sites. With Seal-in-Search, visitors can immediately see in their search results organizations with the Norton Secured Seal installed that met the criteria for safe sites. Since 2004, Symantec reports a 100% upload rate of SSL certificates in the OCSP protocol; when Symantec claims "always on" SSL certificates, Symantec has the track record and the infrastructure to perpetuate its continuous availability claim.

SYMANTEC CERTIFICATE INTELLIGENCE CENTER (CIC)

The Symantec CIC is the management, monitoring, and research center for Symantec's interaction with enterprise customers. CIC helps businesses maintain business continuity and helps prevent certificate expirations.

The protection service has practical value. When the HeartBleed Bug and POODLE vulnerabilities were discovered, Symantec was able to detect the vulnerabilities through the CIC and through other SSL tools. Symantec was able to notify customers and suggested best practice recommendations to begin mitigation against the threats.

The CIC is where customers go to automate certificate installation to minimize manual errors and increase efficiencies.

TECH SUPPORT AND ATTESTATION

Symantec enjoys a strong reputation as a CA of SSL certificates. The reputation is earned through the quality of SSL certificates and the strong certificate management tools.

Symantec and all its brands are in compliance with industry standards and best practices including NIST and PCI DSS 3.0 standards on SSL certificates, and CA/Browser Forum Baseline Requirements. Additionally, Symantec has earned several important accreditations. Symantec is annually audited by KPMG for Certificate Authority Baseline Requirements, EV SSL, and WebTrust compliance. The CIC is certified as SOC2 compliant by KPMG.

Often an enterprise will employ an IT administrator. That person will be responsible for security and business continuity. Symantec has worked with several IT administrators for more than a decade in some cases. All of this enables Symantec to serve as a trusted advisor to customers in selecting the right SSL certificates for their server configurations.

Tech support is the hidden assurance that customers seek when working with a CA. Symantec has the most resources globally to help customers with support issues. Symantec offers customer support in 150+ countries and in more than 20 languages.

CONCLUSION

The prevalent thinking is that the purchase of an SSL/TLS certificate is a casual decision. While the process should be easy for the purchaser, an SSL/TLS certificate involves a secure certificate, a globally secure infrastructure, automated and self-managed tools, malware and vulnerability assessment, proper industry accreditation, and tech support to fill in unexpected gaps in service or coverage. Symantec has taken a concerted and integrated approach to SSL certificates insuring the most secure and best end-user experience on the Internet.

WHAT TO DO NEXT

- Symantec invites potential customers to study and compare SSL certificate products.
  SSL Certificate by Symantec
- The Compare SSL Certificates Page shows what features are included with SSL certificates.
  Compare SSL Certificates, Purchase SSL | Symantec
- Symantec offers an SSL Test Certificate that is free and valid for 30-days.
  Symantec™ Trust Center - 30 Day Trial Period
- The following link describes features and benefits from the Symantec Certificate Intelligence Center.
  Symantec Certificate Intelligence Center | Symantec
- For information about Symantec Secure Site Pro.
  Secure Site Pro SSL - SSL Certificates | Symantec

ENDNOTES

1. Market Share information comes from the Frost & Sullivan ME report Analysis of the Global SSL Certification Market, September 2014.
2. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who invented the first publicly available digital algorithms. The company RSA is similarly named.

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