VeriSign®

WHITE PAPER

How to Offer the Strongest SSL Encryption

Most Web and network security professionals are aware of Secured Sockets Layer (SSL) Certificates and the critical part they play in your comprehensive Web security platform. Yet, many of these same professionals have little or incorrect understanding of an extremely important protocol within SSL, one with the potential to radically alter the level of protection offered to any given Web site's visitors. That protocol is Server Gated Cryptography, or SGC. Using an SGC-enabled SSL Certificate increases the encryption level available to many site visitors and in fact ensures that the most possible site visitors will connect at 128-bit encryption or stronger.

This technical paper details the effect SGC has on the encryption levels your site can offer to its visitors. You will learn which client systems connect at which encryption levels and how to offer the strongest encryption available to each site visitor. Also, you will learn where to obtain SGC-enabled SSL Certificates for your Web site.

Two Levels of SSL Encryption

SSL encryption occurs at two basic levels, which for purposes of this discussion we can think of as the low level of encryption and the high level. Low-level SSL encryption is encrypted at either 40 or 56 bits. High-level SSL encryption occurs at a full 128 or 256 bits. Whether a given SSL session occurs at the low or the high level of encryption depends on both the configuration of the client system and the type of SSL Certificate in place on the Web server. Many client systems are unable to take advantage of full 128-bit SSL encryption unless an SGC-enabled certificate is in place.

The difference between these encryption levels is dramatic. 128-bit encryption offers 2^{88} times as many possible combinations as 40-bit encryption, which is approximately equal to 300 septillion (300,000,000,000,000,000,000,000,000) times stronger. That's over a trillion times a trillion times stronger. The most common form of encryption breaking is "brute force" computation, the inputting of every possible variable into a prompt until the right one comes up. In 1997, 40-bit SSL was broken in about four hours by a college student using this method, and nowadays it can be broken by a hacker with the right skills and a high-end home system in a matter of minutes. If this same hacker were to attack a 128-bit SSL session, it would take well over a trillion years to break that session.

Factors Determining Encryption Level

Exactly which clients will step up to 128-bit SSL encryption and which will not is determined not only by the browser version that client is running but also by the operating system on that machine. Either of these factors can cause a client system to fail to step up. It's important to note that these configuration issues exist entirely on the computer that is visiting the Web site; the server's hardware, software, and operating system have no influence over a given visitor's ability to step up to 128-bit encryption.

Browsers fall into three categories. The first is those that are simply incapable of connecting at 128 bits. These browsers are so extremely old that they were released before the capability was available, and no SSL Certificate in existence can connect to them with 128-bit encryption. These browsers include Internet Explorer versions prior to 3.02 and Netscape prior to 4.02. Clients running these extremely old browsers are the only visitor machines that will ever connect to an SGC-enabled SSL Certificate at less than 128-bit encryption. These obsolete browsers are extremely rare today.

The second category of browsers is still old but not as old as the first. These browsers include Internet Explorer versions after 3.02 but before 5.5 and Netscape versions after 4.02 and up through 4.72. They enjoy 128-bit encryption when connecting with SSL Certificates enabled for SGC and fail to use 128-bit encryption when connecting with SSL Certificates that are not. These old browsers are present on well under half the systems in use today but still have a significant presence in the market.

Finally, we have the newest browsers, Internet Explorer starting with version 5.5 and Netscape versions after 4.72. These browsers are capable of providing 128-bit encrypted sessions for both types of SSL Certificate—so long as the operating system allows it. Some of these browsers also are capable of connecting at 256-bit encryption if the Web server also is capable of 256-bit encryption.

Even among those who are well informed on the subject of Web security, many people don't realize that the client machine's operating system can also cause an SSL session not to step up to 128-bit encryption. In particular, many Windows® 2000 systems will fail to step up to 128 bits unless the SSL Certificate supports SGC. It's particularly important to understand that this security weakness occurs regardless of the version of Internet Explorer running on the client system. Even those computers running the very most recent version of Internet Explorer still fail to connect at 128 bits.

Which systems are they? Any copy of Windows 2000 shipped prior to approximately March 2001 that was not subsequently upgraded with one of several Windows upgrade packs will suffer this limitation. The exact number of affected systems is unknown, but in September 2005, the Yankee Group[1], a leading technology analyst firm concluded that "tens of millions" of client systems will fail to step up to strong encryption in the absence of an SGC-enabled SSL Certificate.

The Only Leading Provider to Offer SGC

VeriSign, Inc., is the leading provider of SSL solutions to offer SGC-enabled SSL Certificates. That means VeriSign can provide 128-bit or stronger SSL encryption—the most powerful money can buy—to virtually every client machine that comes to your site. VeriSign offers SSL Certificates that enable the strongest encryption available to every single site visitor, regardless of browser version and operating system. With SGC-enabled SSL Certificates, you can guarantee that every user of your Web site will connect with the strongest SSL encryption available to them.

Only VeriSign offers you the best possible SSL protection combined with the Web's most trusted security mark—adding up to the top-of-the-line protection you deserve and your site visitors demand. VeriSign offers SGC-enabled certificates in each of its major SSL product lines:

- VeriSign® Secure Site Pro is the most chosen SGC-enabled SSL Certificate on the market today. This individual SSL Certificate is the best solution for Web sites with only one or a few servers requiring SSL protection.
- VeriSign Managed PKI for SSL—Premium Edition is the ultimate SSL solution for the enterprise or any business needing to secure five or more servers—enabling management and instant issuance from a single point. The unbeaten SSL protection of Managed PKI for SSL—Premium Edition is part of what makes it possible for over 93 percent of the Fortune 500 and the world's largest banks each to choose VeriSign SSL as a critical component of their comprehensive online security plan.
- VeriSign Managed PKI for Intranet—Premium Edition offers the strongest SSL encryption available especially for corporate intranets.

Can You Afford Not to?

In this time of increasing online security risk, it is important for every Web site administrator to understand the differences between the two types of SSL Certificates and choose the one that offers the strongest protection to the most site visitors. SGC-enabled certificates, like those from VeriSign, are the only way you can protect every SSL session with the strongest encryption available to that site visitor.

After all, do you and the people you do business with online deserve anything less?

To ensure you and your Web site visitors are fully protected with the strongest SSL encryption available, please contact one of our VeriSign SSL security experts for assistance.

Individual Certificate Inquiries

Call toll free 1-866-893-6565, option 3, or 650-426-5112, option 3.
Email: internetsales@verisign.com

Multiple Certificate Inquiries

Call toll free 1-866-893-6565, option 6, or 650-426-5115, option 2.
Email: verisales@verisign.com

For more information, please go to *www.verisign.com/products/site*.

Visit us at www.VeriSign.com.

[1]Yankee Group Research, Inc. "Building Blocks of Transparent Web Security: Server-Gated Cryptography." September, 2005.