WHITE PAPER: ENSURING COMPLIANCE IN THE ASIA PACIFIC REGION WITH SSL CERTIFICATES

White Paper

Ensuring Compliance in the Asia Pacific Region with SSL Certificates

Dan Sullivan

Ensuring Compliance in the Asia Pacific Region with SSL Certificates

CONTENTS

For those doing business in Australia, New Zealand, Singapore, or in other parts of the Asia Pacific region, privacy is a significant concern. Businesses holding personal data have a responsibility to preserve the privacy and confidentiality of that data.This task is complex, especially in an era of sophisticated, global cybercrime. Secure Sockets Layer (SSL) certificates can help protect data and meet the demands of privacy laws across the region.

Protecting personal information has become a global concern. Governments throughout the Asia Pacific region have enacted legislation that requires businesses and other organizations to implement practices to protect private and confidential information. These include, for example:

- Privacy Act of Australia
- Privacy Act of New Zealand
- Personal Data Protection Act of Singapore
- Act on the Protection of Personal Information of Japan
- Personal Data Protection Act of Malaysia
- Official Information Act of Thailand

The details of national legislation vary, but it is prudent to implement best practices that address the major requirements of privacy legislation. Such legislation may be based on several principals, such as:

- Collection of information from individuals
- Manner of collection
- Storage and security of personal information
- Access to personal information
- Correction of erroneous personal information
- Limits on the use of personal information

Protecting privacy is a complex, multifaceted operation that requires multiple security controls, especially encryption. To appreciate the need for the various controls, it might help to review the most prominent threats to privacy.

Threats to Privacy

Although there will always be the risk of individuals seeking private information about others, the most significant threats come from organized institutions including cybercriminals, industrial espionage agents, foreign governments and non-state actors.

Cybercrime has evolved into a global threat that has reached the sophistication of large-scale commercial markets. Many of the same characteristics found in modern markets, such as specialization of labor and services, brokering, and support for financial transactions, are seen in organized cybercrime.For example, an attacker might purchase malware from a developer specializing in identity theft software, hire an attacker to breach a target business to install the software, and then sell identities collected using online auctions open only to other cybercriminals.

Businesses can be the target of industrial espionage, especially if the business has valuable intellectual property that can be stolen electronically. One major telecommunication equipment manufacturer went bankrupt, in large part, due to long-term industrial espionage that left the company with “damages that are incalculable” (Source: Security Affairs, “Nortel, from Industrial Espionage to Bankruptcy”).

Recently revealed actions by nation states indicate that governments are willing to use sophisticated methods to gather information they consider ‘in their national interest.’ Similarly, non-state actors such as hackactivists can threaten the confidentiality and integrity of systems housing personal information.

Together, this ensemble of cybercriminals, industrial espionage actors, nation states, and non-state actors present a constant and sophisticated threat to maintaining privacy. Fortunately, there are measures businesses can take to protect customer information and ensure compliance with privacy regulations.

Encryption: Essential to Protecting Privacy

In spite of security controls that are put in place to protect infrastructure and prevent communication intercepts, servers can be hacked and communications intercepted. Perhaps the single most important control to protecting privacy is encryption. If a device or network were compromised, an attacker would have access only to encrypted data. This data is essentially useless because there is no practical way to decrypt strongly encrypted data without the encryption keys. Businesses and organizations must be sure to encrypt both data in motion and data at rest. In addition, they must keep in mind two attributes of encryption technologies: their strength and the time required to encrypt and decrypt messages.

Strength and Efficiency of Encryption

The strength of an encryption method is dependent on the algorithm used and the length of the key. There are a variety of encryption algorithms available, but older algorithms that use short keys are no longer reasonable protection options. Some of these can be cracked using brute-force searching on readily available computers. Modern encryption algorithms that provide strong encryption cannot be practically cracked with available computing resources.

When implementing encryption, best practice is to use leading-edge encryption technologies, such as elliptic curve cryptography (ECC).Like other encryption methods, ECC is based on the need to solve an intractable mathematical problem to crack an encryption code. The advantage of ECC is that strong levels of encryption can be realized with keys that are shorter than some other approaches. This setup can lead to more efficient encrypting and decrypting of messages. This consideration is an especially important factor when large amounts of data are encrypted.

Perfect Forward Secrecy

Data that has been encrypted by a strong encryption algorithm can be decrypted only by someone with the decryption key for that message. Thus, if two people are sending encrypted messages and they use different keys, someone with one of the keys cannot decrypt messages that need the other key. This setup provides a level of protection in case one of the keys is compromised.

In a similar way, if one person sends multiple messages and re-uses the same key, there is a chance that an attacker could gain access to one key and decrypt multiple messages. For this reason, businesses and organizations must look for support of perfect forward secrecy. This property of encryption systems guarantees if one message is compromised, there is not a risk that other messages could be compromised using knowledge gained from the initial attack (see Figure 1).

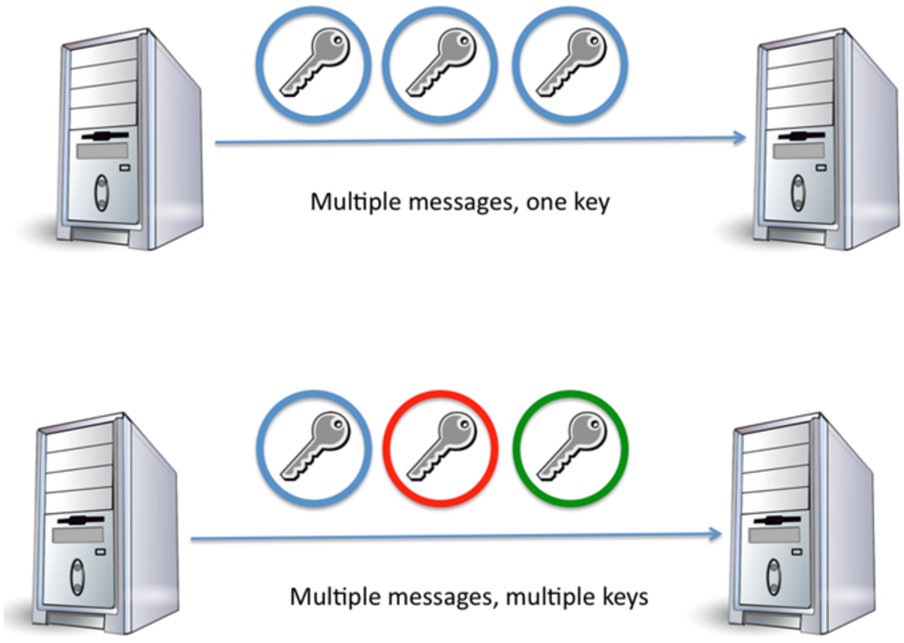

Figure 1:Perfect forward secrecy uses multiple keys to mitigate the risk that one compromised key can leave multiple messages vulnerable to decryption.

In addition to using the best encryption technology, businesses must be sure to implement practices that protect the integrity of encryption operations.

Implement Best Practices that Include SSL Certificates in Compliance Regime

Protecting the privacy of customers and maintaining compliance with privacy regulations is helped by several best practices. First, use SSL certificates from trusted vendors. Some vendors require minimal proof of authentication while others have had their infrastructure hacked. Give preference to well-established vendors with strong track records of protecting their own infrastructure.

Ensure all servers with confidential and private data are protected by SSL. Doing so will enable encryption for both data at rest and data in motion.

Also, implement management controls that keep certificates up to date. Expired certificates can create error conditions and applications and may prevent customers from accessing your applications.

Finally, consider always-on SSL, a best practice advocated by the Online Trust Alliance. Always-on SSL is the practice of using a secure SSL channel for all communications from the time users log onto an application to the time they leave.

A World of Privacy

Privacy is a global concern and governments in the Asia Pacific region have passed legislation that requires businesses and other organizations that collect private information to implement procedures to protect that information. Threats to privacy are diverse, constant, and sophisticated. Encryption and authentication enabled by SSL technologies is an important component of a comprehensive set of security controls that can help your organization maintain compliance with relevant regulations.

More Information

For specific country offices and contact numbers, please visit our website:
http://www.symantec.com/en/aa/globalsites

For product information in the Asia Pacific region, call:

Australia:	+61 3 9674 5500
New Zealand:	+64 9 9127 201
Singapore:	+65 6622 1638
China:	+86 1061950164
Hong Kong:	+852 30 114 683
Taiwan:	+886 2 2162 1992
India:	+91 11 41207680

Or email:
New Zealand / Australia: ssl_sales_au@symantec.com
All other Asia: ssl_sales_asia@symantec.com

Symantec
Symantec Website Security Solutions Pty Ltd
3/437 St Kilda Road, Melbourne,
3004, ABN: 88 088 021 603
www.symantec.com/en/aa/ssl-certificates

Symantec™

Norton™ SECURED
powered by Symantec

UID: xxx/09/14