White Paper

Enhancing Website Security with Algorithm Agility

Symantec™

Enhancing Website Security with Algorithm Agility

Contents

Introduction

Business owners require flexibility and scalability in their efforts to build trust and protect online sites and transactions from Hackers. Hackers are constantly developing more sophisticated methods to breach security protections and inflict damage on a business or its customers.

Responsible business owners have long known to protect their online presence through the use of SSL certificates provided by trusted third party Certification Authorities (CA). The use of an SSL certificate allows authentication of the web server, the transmission of sensitive information, and a recognized and trusted sign of security to customers. SSL Certificates have traditionally relied on encryption using public and private keys based on the RSA algorithm. While these keys remain secure, increasing threats from ever more powerful computers prompted the National Institute of Standards and Technology (NIST), among others, to call for additional strengthening of online encryption.[1]

With this need for additional security in mind, and to ensure that business owners can customize their protection to the needs of their business, Symantec, the most trusted name in SSL Certification,[2] has introduced algorithm agility as part of its SSL certification process. This means businesses now have the ability to choose between certificates that provide protection based on the RSA algorithm, on two alternative algorithms, ECC and DSA, or to generate certificates for all three to install on a server. This flexibility allows business owners to provide a broader array of encryption options for different circumstances, infrastructure and customer or partner groups.

This paper examines algorithm agility, how it fits into the current and evolving security landscape and how your business can enhance online security through a more flexible, scalable approach to SSL certification.

Encryption Today

Transport Layer Security (TLS), and its predecessor Secure Socket Layer (SSL) protocols, remains the industry standard for website authentication and protecting information in transit. Used by websites and browsers, TLS allows for the authentication, compression, and encryption of data passing between a client (end user) and a server, ensuring that hackers cannot access data while it is being sent.

Users know that they are accessing a website or page protected by TLS when "http" in the address line is replaced with "https," and a small padlock appears in the status bar. Such secure pages require the use of SSL certification to enable the encryption of information that is transmitted to or from a secure web server. The vast majority of SSL certificates today rely on keys generated by and signed with the RSA algorithm.

The RSA algorithm remains an effective encryption option. However, the length of the keys will continue to grow exponentially. Online communities have noted the ability of hackers using powerful computers to potentially crack keys approaching

[1] http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf
[2] Symantec US Online Consumer Study, February 2011

1024 bits. NIST has therefore recommended that, by the end of 2013, Certificate Authorities should not issue any new SSL/TLS certificates with RSA public key sizes smaller than 2048 bits.[3]

At the same time, alternative algorithms for encryption and signing have been adopted by the federal government, which has issued guidelines based on Elliptic Curve Cryptography (ECC) and Digital Signature Algorithms (DSA).[4] Already binding on the Federal Government, the new NIST Suite B guidelines and recommendations are also usually adopted as best practices by commercial businesses.

Certificates signed with the RSA algorithm have been in widespread use for many years, but algorithm agility, based on the NIST guidelines, allows businesses to choose to implement certificates signed with three different algorithms: RSA, DSA and ECC. The design of TLS allows different algorithms to work either alone or side by side, so with algorithm agility, business owners can choose the public key algorithm, or combination of algorithms, that works best for their online presence and infrastructure.

How Algorithms are Changing

While all three public key cryptography systems are secure, efficient and commercially viable, they differ in the kind of mathematical problem on which they are based. Not only does this affect how vulnerable they are to brute force attacks often used by hackers, but it can also lead to differences in the size of the keys generated by the algorithm to provide a certain level of security. NIST provides guidelines for minimum sizes of the different keys according to the level of security required.

	Minimum size (bits) of Public Keys			**Key Size Ratio**	**Protection from**
Security (bits)	DSA	RSA	ECC	ECC to RSA/DSA	Attack
80	1024	1024	160-223	1:6	Until 2010
112	2048	2048	224-255	1:9	Until 2030
128	3072	3072	256-383	1:12	Beyond 2031
192	7680	7680	384-511	1:20	
256	15360	15360	512+	1:30	

Table 1: National Institute of Standards and Technology Guidelines for Public-Key Sizes

The chart above clearly shows that the size of RSA and DSA keys grows at a much faster rate than those based on ECC when faced with increasing security requirements. This is important because longer keys require more storage space, more bandwidth to transmit, and potentially, more processor power and time to generate the keys, encrypt, and decrypt with them.

[3] http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf
[4] http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf

The RSA algorithm is, and is likely to continue to be, widely used for some time, and for most TLS Certificates, RSA will remain the algorithm of choice for Web transactions. However, as security demands increase, and use of mobile devices continues to expand, there is a growing need for a more flexible encryption landscape where business owners can customize the kind of protection they get to the needs, scale and technological configurations of their particular businesses.

An increasing number of tablets, smart phones, and other mobile devices are driving more traffic onto the web. This is great for business, but can present a challenge for the number of total simultaneous connections to a single site. Algorithm agility can provide a scalable solution without sacrificing security.

A Closer Look at the New Algorithms

If the options for encryption are expanding, what changes are made to the levels of protection available to businesses, and how will algorithm agility, the ability to choose between three different algorithms, affect SSL certification?

First, let's take a closer look at the algorithms.

Digital Signature Algorithm (DSA)

DSA is a discrete logarithm system. It was developed by the National Security Agency in 1991 as an alternative to RSA and is the federal standard for digital signature.[5] The DSA algorithm provides the same level of protection and performance as the RSA algorithm for similar key sizes, but uses a different mathematical algorithm for signing, and the detection of any alteration to a transmitted message.

Although key sizes are identical to RSA, key generation and digital signature using DSA is faster. Key verification is slightly slower.

DSA is also compatible with most servers, and because it is already a federal standard, using an SSL certificate that supports DSA makes it easier for businesses to meet the requirements of government contracts.

Elliptic Curve Cryptography (ECC)

The NIST Suite B recommendation that Certificate Authorities increase the minimum key size associated with RSA supported SSL certificates demonstrates that increasingly sophisticated security threats will drive the requirement for ever larger RSA keys. As Table 1 shows above, at a certain point, the RSA key size for the security required simply becomes unwieldy, increasing the amount of computing power, bandwidth for transmission and time required for the encryption and decryption operation. It's still secure, but less efficient.

Unlike RSA and DSA, ECC algorithms are based on elliptic curves over finite fields, a much more difficult mathematical problem for hackers to attack using simple brute force methods. Using RSA and DSA algorithms, the defining factor for how secure the encryption can be is key length.

[5] http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf

With ECC, the nature of the mathematical problem at its core means that as key size increases, its decryption operations become more difficult at a faster rate than those of RSA. This means that a shorter ECC key is more difficult for a hacker to break than the same length of RSA key and can provide the same or better security coverage than a much longer RSA key. Key sizes for ECC increase linearly instead of exponentially, so as guidelines change their efficiency increases.

Algorithm Agility — Choosing the Right Algorithm for your Needs

While ECC is already embraced by federal agencies, ECC is not ubiquitous in terms of adoption, allowance, and availability across all browsers and servers. For businesses, this means that ECC may not, if used as the only encryption algorithm, be the right solution for your particular mix of hardware and devices.

When looking at the customer side, ECC is a relatively new technology for mobile and browsers, so it may not yet be easily available to all of your customers. If the customer device or browser does not support a particular algorithm, that customer may not be able to complete a transaction. This means that ECC by itself may not be the best choice for the SSL certificate for, by example, a retail site where customers need to feel confident that they can make purchases easily and securely. However, a business using multiple certificates; DSA and RSA, ECC and RSA, or all three at once; increases their coverage.

Several factors will help you decide which algorithm, or combination of algorithms, in your SSL certificate best meets the needs of your business. While it is highly likely that RSA will continue to be used for some time, algorithm agility opens up new options. The option to choose SSL certification based on different algorithms allows business owners to extend their online security, easily meet the needs of government clients and partners, and tailor security protection to their business requirements in a way that has not previously been possible.

The first factor for business owners or IT managers to consider is the organization's current Web server standards. Some web servers can handle RSA, DSA or ECC, and can be configured to use all three types of certificate for one domain name on a single Web server. Others can handle RSA or ECC but are limited to only one certificate per Web server.

TLS is also used for encryption between email servers and other services, and the internal tools, scaling, and architecture for these services would need to be considered.

Second is the tradeoff in speed of authentication between the algorithm types. RSA is faster on the client side of authentication, and ECC is faster on the server side. RSA signatures also can be verified faster than ECC signatures. The usage of each key type will depend greatly on the type of transaction intended. Factors to consider here include the processing power of the end device, storage space, bandwidth, power consumption and how widely the algorithm is adopted by your customers and their client devices or browsers.

The number of expected connections may also play a factor in decision making. Depending on web server configuration, servers may be able to handle more concurrent connections with an ECC certificate than an RSA certificate. An organization must consider their needed balance between safety, user experience, and IT costs in network processing.

The last consideration is the identity of your customers or partners. DSA and ECC are embraced by many government agencies and may be required in interactions with them. This could include government contracts and sub-contracts, and information exchanges with governmental branch entities.

In a best case scenario, an organization would be able to install all three certificates on their transaction server. Configured properly, a server could then accept any request from an end point, avoiding risk, and providing 100% client coverage.

Next Steps

In order for customers to truly realize all of the benefits of the enhanced security offered by new algorithms, DSA and ECC support will have to become more widespread, especially in the mobile environment that is processing more and more of our daily online life.

This may also lead to changes in the visual cues we are accustomed to on web browsers. As yet, there is no standard for mobile or tablet browsers equivalent to the trusted HTTPS and padlock indicators, as well as the Extended Validation green bar we now see on web browsers.

In the meantime, Symantec’s algorithm agility approach provides businesses with an easy and effective transition. Symantec customers now have the option to choose SSL certificates that use both the traditional RSA algorithm and either DSA or ECC algorithms for enhanced security.

Conclusion

Security demands will increase and hacker attempts will become more sophisticated and powerful, but security measures are improving alongside the threats. Algorithm agility will be of increasing value to businesses, allowing owners and IT departments the flexibility and scalability they need to tailor protection to the needs of their customers and their businesses.

Symantec has made it easy to get started. Our popular SSL certificates now include DSA or ECC algorithms alongside the standard RSA algorithms. Integrating the new algorithms into SSL certificate products provides a convenient way for businesses to improve and enhance their online security in partnership with the most trusted Certificate Authority in the world.

More Information

Visit our website

http://go.symantec.com/ssl-certificates

To speak with a Product Specialist in the U.S.

Call toll-free: 1(866) 893-6565 or 1(650) 426-5112

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

Symantec Corporation World Headquarters

350 Ellis Street
Mountain View, CA 94043 USA
1 (866) 893 6565
www.symantec.com