Managing certificates during a time of key size migration can be difficult. Website or production outages can be costly and have a negative impact to business. This guide aims to help educate and inform users of TLS/SSL certificates about the upcoming change in key lengths and tips on managing their transition to using stronger SSL certificates.

Background

Until the recently, the RSA algorithm, first publically described in 1977 has been the only algorithm available for commercial digital signing certificates. It remains the de facto standard although now commercial certificates based on the DSA and ECC algorithms are now available. The larger the key in an RSA certificate the more difficult it is to compromise the encryption. As raw computing power increases over time it becomes possible to factor or crack smaller sized RSA keys. Seventeen RSA key sizes have been factored since 1991. Most recently most of the industry has standardized on certificates with 1024-bit RSA keys. However, industry experts warn that the oft used 1024-bit RSA key size is now at risk of being compromised by cyber criminals. As a proactive measure, NIST has recommended that 1024-bit RSA certificates be eliminated and replaced with 2048-bit or stronger keys. As a result of the NIST recommendation, the Certification Authority/Browser (CA/B) Forum, created to develop best practices within the SSL/TLS industry, created a mandate to bring the 1024-bit RSA key size to end of life by December 31st, 2013.

The Responsibility of a CA

All responsible Certificate Authorities (CAs) should be informing their customer base of this regulation change and assisting them with their migration to a more secure key-size. Since 2011, Symantec has been actively communicating with customers to ensure all stakeholders associated with each 1024-bit owned certificate are informed of this transition. For more information on this issue stakeholders are encouraged to visit the Symantec 1024-bit information site. Due to the industry’s end-of-life mandate on 1024-bit certificates Certification Authorities have the difficult requirement to revoke 1024-bit RSA certificates that expire after 12/31/13.
Complications for End Users

Owners of 1024-bit RSA end-entity certificates fall into two categories. The first have certificates expiring before the mandated deadline. In this case, any new certificates issued this year must be based on a stronger algorithm key size such as 2048-bit RSA, 2048-bit DSA or 256-bit ECC. The second group has certificates with 1024-bit keys expiring after the 12/31/2013 deadline. These certificate holders must revoke and replace their certificates with certificates based on stronger keys. Symantec recommends doing this before October to avoid IT blackout periods and the holiday shopping season when online traffic is at its highest. The biggest challenge comes when users are not aware that they are still using SSL certificates based on 1024-bit keys or are unaware that their CA will be automatically revoking any 1024-bit SSL certificates that expire beyond the deadline date sometime before the end of 2013.

ECC as a Faster Alternative to 2048-bit RSA

Doubling the key size of a certificate will affect system performance. There is an alternative SSL technology now available. Symantec now offers SSL Certificates based on the Elliptic Curve Cryptography (ECC) algorithm. These ECC based certificates use a 256-bit key, so they require fewer CPU resources, less network bandwidth and deliver faster response times. Symantec began work on ECC in 2005 when it began releasing Elliptic Curve Cryptographic (ECC) roots into the major browsers. Because different math is involved a 256-bit ECC certificate is substantially stronger than a 2048-bit RSA certificate.

Testing has shown a decrease in CPU usage when using a 256-bit ECC certificate compared to its 2048-bit RSA contemporary. Symantec is the only CA to offer an ECC certificate on a complete ECC chain from root to intermediate to end entity and is available on any Premium SSL offering. Check out Symantec’s SSL web site or speak to a representative today at 1-866-893-6565 to learn more about ECC certificates.

Fact: ECC is 10,000 times stronger than 2048-bit RSA

What End-Users Must Do

1. Test your system with a valid trial certificate with a 2048-bit key to ensure your system can handle a larger key size (some older environments can’t). You can download a trial certificate at go.symantec.com/ssl-trial.

2. Find all the 1024-bit certificates within your environment. If you have a complex environment with many SSL certificates, you may consider using a certificate discovery and management solution. Symantec’s Certificate Intelligence Center can help discover and manage all certificates regardless of who has issued the certificate. In addition you can also automate the transfer of certificates into Symantec SSL certificates. For customers that only manage a few domains/servers you may also check individual domains secured by Symantec, GeoTrust, Thawte or RapidSSL certificates with the Symantec Certificate Checker.

3. Identify the validity period for your certificate to create your plan of action. Certificates that are expiring in 2013 will need to be upgraded during your normal renewal process. You will need to revoke and replace any certificates expiring after the end of the year. Make sure you do this before your CA has decided to terminate this pool of certificates. Your CA certainly does not want to surprise you with this activity.

4. Generate a new Certificate Signing Request (CSR) for a 2048-bit RSA key size. Symantec offers assistance on their CSR help page. Use this CSR to enroll for your new stronger certificate.

5. If you have a certificate that expires in 2014 or later you will need to revoke and replace that certificate before the CA/B Forum deadline of 12/31/13 or when your CA is scheduled to revoke certificates expiring in 2014 or later.

6. Once your new certificate has been issued, install the end-entity certificate and any additional intermediate certificates on your server. You can get additional instructions and videos on installation on the Symantec 1024-bit information site.

7. Finally, test your website or link to ensure you have a safe and encrypted connection. There is a good test utility available here.
More information
Visit our website
http://go.symantec.com/ssl-certificates

To speak with a Product Specialist in the U.S.
Call 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 protects the world’s information and is the global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device to the enterprise data center to cloud-based systems. Our industry-leading expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

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