DIGITAL CERTIFICATES

THE BASICS, SWEEPING INDUSTRY CHANGES COMING IN 2018 AND HOW TO BE PREPARED FOR THEM

by Doug Beattie, vice president of product management, GlobalSign

With an incredibly active threat landscape today there are a plethora, and even perhaps overwhelming, number of options to consider to ensure your company's cyber safety. One of the first "basic" items on your security check list should always be to have the proper SSL certificates in place.

SSL certificates offer the strongest encryption to ensure your website is protected. Customers and visitors to your site will be confident knowing their browsing session is safe and that information such as payment details and personal information are secure and encrypted.

Security professionals understand that, among the varying levels of certificates, Extended Validation (EV) certificates are the "gold standard". They activate the browser padlock and https, and shows a company's corporate identity, which assures your customers that you take security very seriously. They also lend more credibility to a website.

All certificates should be obtained from a reputable Certificate Authority (CA). Research carefully and do be wary of lower level certificates, such as Domain Validation (DV) certificates that are free, as some have been linked to dangerous phishing scams.

WHY SSL CERTIFICATES ARE IN THE NEWS NOW

What's got lots of tongues wagging these days is related to the fallout from Google's dispute with Symantec.

This began two years ago when Google engineers discovered Symantec accidentally mis-issued 127 SSL certificates. The issue rose to prominence again in March of this year when Google announced that it had uncovered more concerns with Symantec's certificates, alleging the company had mis-issued more than 30,000 certificates. Then in August, Symantec decided to exit the web certificate business and sell it to Digicert.

The end result is that by mid-April 2018, all Symantec-issued certificates obtained prior to June 1, 2016, will be marked as untrusted by Chrome 66. Then by the end of October 2018, all certificates that are chained to Symantec's pre-December 2017 rooted infrastructure will be untrusted by Chrome 70.

This is an extremely significant development, and will certainly have the people responsible for maintaining secure systems busy as they consider their next steps.

THINKING OF SWITCHING TO A NEW CERTIFICATE PROVIDER?

With the sweeping changes being implemented by Google (and Mozilla by extension), some companies may be considering making a switch to a new SSL service provider.

While it's not necessarily an extremely complex process, it will be necessary to plan this out. It is also strongly recommended you give yourself enough time to determine whether you want to remain with your current CA, or if you do indeed want to jump to a new one.

If you're strongly considering making a switch, following are some important steps to consider.

At the outset, it will be important to survey and access your existing certificates, your company's needs as well as your usage. You should also be inventorying everything so you know what needs replacing once you decide to make a switch. In addition, it will be necessary to identify which of your team members will manage your new account. Making sure you train these individuals on the new GUI (Graphical User Interface) is key, and you should factor any training time into your transition timeline.

Also important during the certificate authority switch is API integration. If you have one with your current CA, there will need to be a similar integration with your prospective new CA who should have satisfactory API documentation, and be able to provide support and guidance throughout the on-boarding process.

Another critical element in this process will be estimating the costs involved of a switch. You should be thinking about everything from capital and operational expenditures to annual costs, product definitions and any set-up fees you'll incur with the new CA.

During this process you should insist on a solution that includes comprehensive SSL certificate management. This service helps customers discover, inventory and manage all SSL certificates across their network and cloud services. Most CA's today offer this to reduce risk, respond to threats but also to control SSL costs.

Finally, when comparing managed SSL providers, be sure you place an importance on the fact that you are essentially picking a business partner, not just a product, as this is a relationship that goes well beyond just its delivery. Your organization will have a dependency on the CA long after they have issued your certificates.

Your prospective new CA should also be able to provide you with the highest security, feature-rich SSL Certificates. They should also be able to provide sound advice on security initiatives, take your business needs into consideration when making recommendations, and provide you with tools in order to verify that your web server configuration has been optimized to guarantee maximum security.

It's been a very active year for the certificate market. One major player is exiting and Google Chrome has been vocal about some very significant changes it will be implementing next year. Now is a good time to consider all your certificate options, and map out what makes the most sense for your company so you're not caught off guard in 2018.

About the Author

Doug Beattie is the Vice President of Product Management at GlobalSign. He is responsible for defining, positioning and launching all SSL-related products. Prior to joining GMO GlobalSign, Mr. Beattie was Principal Systems Engineer at General Dynamics where he was the lead architect responsible for driving and building a smart card management system issuing over 500K PKI-enabled smart cards for the US government. Prior to joining General Dynamics, Mr. Beattie was the Director of Product Management at GeoTrust where he led the SSL line of business from their first SSL certificate sale through the successful acquisition of the business. He has also held positions at CyberTrust Solutions, a PKI and e-Security firm, Securant Technologies, an access and privilege management product, and GTE Government Systems Corporation. Doug can be reached online at doug.beattie@globalsign.com and at http://www.globalsign.com/