14 August 2017

Symantec to Sell Web Certificate Business? Certificates to Start Being Distrusted in August

How will this impact customers and partners and what should you do right now?

While it may only be a rumor right now that Symantec is exploring the sale of its web certificate business, the news is being picked up by very legitimate news sources stemming from a Reuters article that broke on July 11th 2017. Much of this rumor is being fueled from the very public fight Symantec is having with Google over mis-issued SSL Certificates. One of my favorite news headlines: Google takes Symantec to the woodshed for mis-issuing 30,000 HTTPS certs.

At the time the news hit about the mis-issued certificates, Google laid out some extreme measures, including Chrome's non-acceptance and trust of Symantec certificates for a 9 month period. Symantec is an SSL Certificate market leader and this could render hundreds of thousands of websites and servers as being insecure and not trusted. Not a good thing when many of Symantec's customers are large financial and health care organizations. This alone would cause a huge disruption for customers and commerce in general.

The latest development: Google will now start the process of distrusting Symantec certificates on August 8th 2017. That's in just a few short weeks. This is not only affecting Symantec customers, but their partners as well. In a quick search of the Symantec website, I found 626 partners that offer Symantec SSL Certificates as part of their business. To some partners, offering Symantec SSL Certificates is a main chunk of their business. Additionally, those partners' customers trust these partners for their technology needs including security and SSL requirements. As a Symantec partner, you cannot risk losing any part of your revenue stream or customer base.

And, with the rumor of the sale, what are customer and partners to do in order to protect their customers' business? FACT: If your Symantec certificates are no longer trusted, this will impact your business…PERIOD! Should you be worried? YES! But if you act fast, there are easy steps you can take to ensure security, business continuity and positive customer experience.

What can you do right now?

Whether you are a Symantec customer or a partner, you need to start investigating other SSL providers RIGHT NOW and SWITCH to a new SSL vendor as soon as you can. Of course, I will recommend GlobalSign and I will give you the reason for doing so:

1. Service – Support – Platform – Did We Mention Service?

In a previous blog article, 5 Reasons to Switch Your SSL Provider or Certificate Authority, we highlighted reasons like cost and value, features and benefits, service and support, comprehensive lifecycle management, and trust and compatibility. When it comes to SSL Certificates, the basics are pretty much the same. The true difference comes in the platform, services, type (DV, OV, EV) and then support personnel to issue, manage and ensure you don't have downtime.

You should also look at a trusted Certificate Authority (CA). GlobalSign has been a public CA since 1996, is WebTrust audited, and is a true "one stop PKI shop" - our feature-rich Managed

PKI platform supports not just SSL needs, but also certificates for user, machine, and device authentication, mobile devices, digital signatures for documents, code signing, and S/MIME email encryption and digital signatures. We are active members in the CA/Browser Forum and CA Security Council. And, with more than 25 million certificates relying on our trusted root, we are a CA that our customers trust.

2. Switching SSL Certificates to GlobalSign is Easy and Cost Effective

We make SSL easy from the very beginning. Our Managed PKI platform offers complete certificate lifecycle management, including reissuance and revocation, delegated user administration, and robust reporting and auditing capabilities. All domains via GlobalSign's managed certificate platform are pre-vetted so certificates can also be issued immediately after they are requested. You can also use existing ACME Client software to automate SSL Certificate provisioning and installation. Our ACME implementation supports higher assurance OV and EV Certificates with flexible validity periods.

GlobalSign is the only CA that offers complimentary SSL Management tools, like our Certificate Inventory Tool, to help discover all your certificates. You will want to make sure you can find and replace all of your Symantec SSL Certificates. Also included with our services, we offer the SSL Server Test to help configure servers correctly and to find potential weaknesses and vulnerabilities. This ensures that all of your certificates are installed and configured correctly the first time.

Additionally, we offer flexible business terms to accommodate organizations of all sizes and structure, including unlimited issuance plans, pay as you go, SAN licenses, and bulk deposits. All SSL Certificates come with unlimited server licensing, so you can install across as many devices as needed. And, with worldwide local language service and support, we can accommodate organizations on a global scale.

There are also discounts for switching that can include 30 percent off, time remaining on your existing certificates will be added to your new GlobalSign certificates and 30 additional days of validity – up to 27 months max.

3. What Steps Are Involved in Switching to GlobalSign?

In a previous blog written by Doug Beattie, Vice President of Product Management for GlobalSign's SSL products, he breaks down how a switch can happen in four easy steps. Read the Complete Guide to Switching your MSSL CA Provider. It's time to get started now before the August 8th deadline and we can help you along the way. Contact us today and our SSL Certificates experts will assist you.

by Christian Simko