Switching Managed SSL Service Providers

Demystifying the process and setting expectations

GLOBALSIGN WHITE PAPER

TABLE OF CONTENTS

INTRODUCTION

Switching to a new Certificate Authority for your SSL certificates is not a simple process, but it is not nearly as complicated as your incumbent CA may suggest. The key to success is setting expectations and preparing yourself and others for what's involved, in terms of resources and costs.

This white paper walks through the process of switching to a new CA, from the initial step of understanding your current environment through figuring out what needs to be done and estimating the costs.

STEP 1 – SURVEY WHAT YOU HAVE

When considering switching managed SSL service providers, your first step is to survey the existing SSL usage and environment. You need to know what you currently have to set reasonable expectations for the costs and the time involved in switching.

INVENTORY YOUR CERTIFICATES

First, determine the location of existing certificates so you know what you need to replace after making the switch. Large enterprises often have many active SSL Certificates in their environments. If you don't find all certificates during the transition, they could expire, leading to lapses in coverage, possible network outages, and issues with compliance.

"Service outages due to unplanned certificate expiration impact service availability, SLAs, brand confidence and trust by customers, partners, and other relying parties, and can lead to noncompliance with regulatory or other requirements." [1]

How you get the certificate inventory depends on your organization's order history and whether you use multiple CAs.

CERTIFICATES FROM MULTIPLE CAS

You might have certificates from more than one CA for many reasons, including:

- Multiple individuals or departments purchasing certificates separately from different service providers
- Multiple CAs as the result of mergers and acquisitions

Working with multiple CAs can make it difficult to get an accurate inventory. Fortunately, you can use certificate discovery tools to index your network and locate all existing certificates, regardless of the issuer. This gives you a complete list to reference when it comes time to migrate to a new CA.

[1]Gartner, X.509 Certificate Management: Avoiding Downtime and Brand Damage, Eric Ouellet & Vic Wheatman, 4 November 2011

CERTIFICATES FROM A SINGLE CA

If you are confident that all of your existing SSL Certificates were issued from the same CA, download a list of your certificates from that account. This gives you a record of all previous purchases, without having to rely on the old account throughout the migration process.

IDENTIFY ADMINISTRATORS

Identify which team members will manage the new account. You will need to make sure to train these individuals on the new GUI. Factor the training time into the transition timeline.

IDENTIFY SERVERS & APPLICATIONS

Evaluate the number and type of servers and applications you have certificates installed on, so you know what to expect when it comes time to do the actual switch. For example, depending on the type of server, you may need to do manual root replacements.

STEP 2 – DETERMINE WHAT NEEDS TO BE DONE

Once you know what you're working with, you can take a look at the logistics behind switching.

Often organizations are deterred from switching CAs because of misconceptions about how painful and time-consuming the process is. However, when you scope exactly what is involve you may discover that it is quite feasible.

Let's take a look at what actually needs to be done to make the transition as smooth as possible.

LEARN THE NEW GUI

You will need to include training time as you plan your switching timeline. This is why you need to know how many users you have and their roles and responsibilities. The account administrator may require more training that someone who is only responsible for placing orders.

DECIDE ON A RENEWAL STRATEGY

Before you switch SSL providers, you should devise a plan of attack for handling certificate renewals. When choosing your new CA, you should inquire about their certificate replacement policies. They should be able to accommodate both of the following methods.

TRANSITION MODEL

One option is to approach renewals on an individual certificate basis, replacing each certificate as its expiration approaches. Make sure you have accurate certificate reports and that the responsibility for managing renewals is assigned to the appropriate team member. Using this model, you spend less time installing certificates during the initial switch period, but you need to be diligent about monitoring expiration dates until all certificates have been renewed under the new management account.

"RIP & REPLACE" MODEL

You can also choose to replace all of your certificates at once. Using this approach requires an initial investment of time and resources to replace all existing certificates at once. But you will not have to worry about monitoring old certificates throughout the rest of their lifecycle and you will not have to rely on several management platforms.

Your preferred CA should be able to compensate for any remaining time left on a certificate by extending the validity period of the new certificate.

IDENTIFY INTERNAL VS. EXTERNAL USAGE

Certificate features and security levels vary by CA. Review the certificate offering from your new CA and identify which products you need for your usage requirements

- For public-facing sites, the SSL Certificate proves to the site visitor that the site is legitimate and can be trusted. Secure these sites with a quality certificate from a reputable brand.
- For internal sites, where you really just need encryption capabilities, you can use a more basic certificate.

SCOPE ANY API INTEGRATION

If you use an API integration with your current CA, you will need to create a similar integration with your new CA.

Your preferred CA should have adequate API documentation and provide support and guidance through the onboarding process. Be sure to allot time to configure the new API into your project timeline.

"Use the most publicly trustworthy, well-known brand-name certificate providers for external uses, particularly those directed to risk-sensitive customers." [2]

"Shop on price when PKI will be used only to support SSL/TLS encryption, but recognize the requirements to manage encryption certificates in the long term." [2]

[2]Gartner, How to Succeed in Revamping Your PKI Program, Brian Lowans & Eric Ouellet, 4 May 2012

DON'T WORRY ABOUT THESE MYTHS

Organizations are often deterred from switching CAs by misperceptions. These are the most common.

"ROOT & ICA DISTRIBUTION IS TOO DIFFICULT"

One common excuse for staying with your incumbent CA is that you don't want to go through the cumbersome process of distributing the new CA's roots and ICAs. In reality, this process is fairly routine, although it may affect your schedule.

- If your IT change management policies allows you to install roots at any time, you can install the roots when you install the end entity certificate. Most vendors provide all the necessary certificate chain components with the end entity certificate fulfillment process.
- If you have a stricter change management process, distributing the ICA could affect your switch timeline. For example, if you have specific maintenance windows in which to perform IT changes, you may need to schedule your CA switch to accommodate this.

Because SSL/TLS Certificates are based on a common standard (i.e., X. 509 v3), the process of requesting and installing certificate chain components is *exactly the same* from one vendor to the next.

"UPDATING OCSP PATHS MANUALLY IS PROHIBITIVE"

Another common myth about switching CAs is that you will need to manually replace the CRL and OCSP paths when you start issuing certificates from the new CA. If your organization only uses certificates on webservers, you do not need to worry about this.

Every issued SSL Certificate must contain a link to the issuing CA's CRL; you don't need to do anything for this. If you have non-webserver instances, you may need to manually replace the revocation path. This is why it is important to know how your certificates are being used.

STEP 3 – ESTIMATE THE COST

Once you have an idea of what's involved in switching providers, you can scope the costs.

CAPITAL EXPENDITURES

One-time capital expenditures may include a certificate discovery tool, certificate management services, and API integration efforts.

CERTIFICATE DISCOVERY TOOL

If you have certificates from multiple CAs, you may want to use a certificate discovery tool to inventory certificate usage. This service is often bundled with the Certificate Management Services discussed below at no extra cost.

CERTIFICATE MANAGEMENT SERVICES

Your preferred CA should offer a SaaS-based certificate lifecycle management platform that will allow account managers to order, renew, and issue certificates, as well as perform other management functions such as billing and reporting.

If your organization handles a large number of certificates, employs a multi-vendor strategy, uses self-signed certificates, or is looking for added convenience and automation while managing SSL Certificates, you may want to invest in additional onsite software for key management. These services combine the inventory function with the ability to provision certificates, linking directly with the APIs from leading CAs using pre-configured "connectors." You can manage certificate lifecycle (e.g., certificate issuance and replacement) from a single platform, without logging into each CA's management system.

"Organizations with roughly 200 or more documented X.509 certificates in use are high-risk candidates for unplanned expiry and having certificates that have been purchased but not deployed. They must begin a formalized discovery process immediately." [1]

These services can also help with compliance by scanning all certificates on the network for cryptography best practices, such as key sizes and hashing algorithms. They can alert you to any certificates that do not meet security standards, and let you replace them easily within the service.

EXISTING API INTEGRATION

If you use an API with your existing CA, factor in the development costs needed to update your code to integrate the new CA's API.

[1]Gartner, X.509 Certificate Management: Avoiding Downtime and Brand Damage, Eric Ouellet & Vic Wheatman, 4 November 2011

NEW API INTEGRATION

Many CAs offer API integration that you can use to automate certificate management, including

- Automating certificate issuance
- Ordering via internal portals
- Maintaining granular usage reports

If you want to automate these capabilities, discuss your desired workflow and functions with your new CA. Factor any internal development time and resources into your first year costs.

OPERATIONAL EXPENDITURES

From an ongoing, operational perspective, you need to factor in the time it will take your account users to get familiar with the new management platform, including setting up reports, delegating responsibilities, etc. Training time will vary depending on the responsibilities of the individual.

ANNUAL CERTIFICATE COSTS

As you evaluate different CAs, you should consider the cost of individual products together with the value they provide in terms of features and functionality, including:

- Any additional fees for reissuance or installing certificates across multiple servers
- Any additional services bundled with the certificate, such as malware and phishing monitoring
- The nature of the certificate itself (for example, issued from 2048 bit root)

Each CA productizes its certificates differently. Review the product line to be sure the certificate meets your needs and does not include unnecessary premium add-ons, such as Server Gated Cryptography (SGC).

"While costs are a major factor, quality of service and bundled services should also be considered." [3]

"Certificate costs should be weighted at 70% of the decision and technical/trust factors at 30%." [3]

[3]Gartner, Evaluating SSL Certificates for E-business, Vic Wheatman, 30 August 2011

STEP 4 – CONSIDER SWITCHING TO GLOBALSIGN

When comparing managed SSL providers, it is important to remember, "You're picking a business partner, not a product. This is a relationship that goes beyond the delivery of a shrink-wrapped product. You have dependency on them long after they've issued you certificates."[4]

In addition to providing you with the highest security, feature-rich SSL certificates, your CA provider should be able to:

- Help you with customized environments
- Advise you on security initiatives
- Make recommendations based on your business needs
- Provide tools to verify your Web Server configuration has been optimized for maximum security

Organizations choose GlobalSign because of its commitment to provide leading digital certificate solutions and being a trusted partner. As one of the largest enterprise-focused Certificate Authorities, GlobalSign employs teams of specialists around the world to support its customers. Its solutions are built around customer needs and industry best practices.

"Security doesn't end at the close of a technology sale. Providers need to delivery ongoing support for products and services that allow their customers to maximize the value of their solutions and increase their effectiveness as the threat landscape changes. As a Certificate Authority, GlobalSign is in the best position to understand website administrators' needs in configuring SSL and remediation of security issues." [5]

THE GLOBALSIGN ADVANTAGE

GlobalSign is constantly investing in making more secure and user-friendly SSL certificates. The company has a history of staying ahead of the curve:

- Using 2048 bit roots since 1998, long before the best practice recommendations
- Was first in industry to introduce certificate revocation services in IPv6

The company continues to update its management platform and develop key partnerships. These innovations and partnerships give GlobalSign important advantages over other CAs.

FASTER PAGE LOADS

Whenever a browser connects to a secure site, the status of the site's SSL certificate needs to be verified with the issuing CA. How long this process (the OCSP response or CRL delivery) takes depends on the efficiency of the CA's infrastructure and the user's location in relation to the CA.

[4] GlobalSign CTO Ryan Hurst as quoted in Salvaging Digital Certificates, Paul Roberts, http://www.darkreading.com/security/application-security/240062664/salvaging-digital-certificates.html

[5] Richard Stiennon, noted security author, speaker and founder of IT-Harvest as quoted in https://www.globalsign.com/company/press/111512-ssl-configuration-checker-provides-guidance.html

GlobalSign has partnered with network performance specialist CloudFlare to benefit from its global infrastructure to deliver fast and reliable certificate status requests. This accelerated OCSP/CRL responses by 6-10 times. Faster page load helps visitor retention and plays a role in improving SEO.

"The combination of our advanced web optimization technology with GlobalSign's forward-thinking approach to SSL will allow both GlobalSign and CloudFlare customers to stay ahead of their competition when it comes to providing a secure, outstanding and fast user experience." [6]

ENHANCED AVAILABILITY

Most CAs rely on a single point of presence for its datacenter to serve OCSP responses and deliver CRLs. If it goes offline, you can experience major disruptions. External visitors will receive security warnings, and internal appliances will be unable to communicate. GlobalSign utilizes 23 datacenter locations worldwide, eliminating such risk.

ONGOING SECURITY FOR YOUR WEBSITE

GlobalSign SSL is more than just a padlock. It keeps your website safe and secure around the clock.

- Online SSL Configuration Checker tests your domain for over thirty of the most common SSL issues and vulnerabilities and provides actionable guidance on remediation
- Phishing alert service through partnership with Netcraft alerts site owners if their sites have been flagged for phishing
- Malware monitoring through partnership with StopTheHacker alerts site owners to both known and unknown malware

"Configuring SSL properly is an important step in realizing the benefits of SSL. However, it's often hard for administrators to find comprehensive guidance on how to accomplish this goal. Our work with GlobalSign is addressing this need and making the Internet a safer place for everyone." [7]

ENTERPRISE CERTIFICATE MANAGEMENT

GlobalSign's SaaS-based Managed SSL service manages certificates across your entire organization. The Managed SSL platform was designed to help enterprises significantly reduce the budget, time and management costs associated with using SSL. With one-time vetting, administrators can issue the full range of SSL certificates, from cost-effective encryption certificates to high assurance EV Certificates for public sites, on demand 24/7/365.

Customize the service to meet your organization's needs, with flexible business terms such as:

- Unlimited certificate issuance licenses
- Bulk deposits
- The ability to add unlimited users, domains and profiles
- Robust reporting and management tools

[6] Matthew Prince, co-founder and CEO of CloudFlare as quoted in https://www.globalsign.com/company/press/110112-cloudflare-partnership-accelerates-secure-web-page-load-speed.html

[7] Ivan Ristic, director of engineering at Qualys as quoted in https://www.globalsign.com/company/press/111512-ssl-configuration-checker-provides-guidance.html

You can integrate the Managed SSL service with Microsoft Windows environments to benefit from the convenience of using Active Directory for certificate provisioning. The integration supports auto-enrollment and silent installs, and reduces the time and operating costs associated with running an on-premise CA.

"Since purchasing a number of SSL Certificates using GlobalSign's Managed SSL, I have found the whole process a joy compared to my previous SSL Certificate provider." [8]

DEDICATED ACCOUNT MANAGEMENT

Every GlobalSign Managed SSL customer has a dedicated Account Manager, one person to contact whenever they need help. Available via phone, web, and email, the Account Manager can assist with product choice, provide support for certificate lifecycle issues, and discuss your organization's upcoming security initiatives.

OPERATIONAL SECURITY

You rely on SSL Certificates to promote your brand reputation, enhance end-user trust, and protect your organization's and site visitors' sensitive information. GlobalSign has earned industry recognition and trust:

- GlobalSign was one of the first CAs to use ICAs and maintain an offline root to minimize the risk of exposing the root CA to attackers. This is now an established security best practice.
- WebTrust is an auditing standard for CAs that issue public certificates. GlobalSign has met annually audited WebTrust compliance continuously since 2001.
- GlobalSign is a founding member of the CA/B Forum and the CA Security Council.
- It is a member of both the Online Trust Alliance and Anti-Phishing Working Group.

In addition to complying with industry best practices, GlobalSign monitors and secures its own infrastructure with appropriate security instrumentation as recommended by third party security consultants.

[8] Richard Sprigg, Dudley Metropolitan Borough Council as quoted in https://www.globalsign.com/resources/case-study-dudley-council.pdf

SWITCHING CHECKLIST

Here is a compilation of the considerations when switching CAs.

Consideration	How GlobalSign Can Help
Learn the New GUI	GlobalSign offers online user guides and tutorials. All customers have a dedicated Account Manager to contact with any questions.
Renewal Method	GlobalSign can accommodate both the transition and “rip and replace” methods. For organizations using the “rip and replace” method, GlobalSign adds any remaining time left on a certificate to the replacement certificate so you don’t miss out on certificate lifetime. Organizations using the transition method will benefit from domain pre-vetting so when the time comes to do the replacement, you will be able to issue the certificate immediately.
Internal vs. External Usage	As the fastest growing CA four years running with over 250k domains relying on GlobalSign SSL Certificates, GlobalSign has the brand reputation expected on public sites together with cost-effective options for internal usage.
Annual Certificate Costs	GlobalSign offers a wide range of SSL certificates to meet every use case. All SSL certificates are 2048 bit, can be installed on unlimited servers, and come with free reissuance. You only pay for what you use and there is no need to purchase tokens or certificate funds.
API Integration	Whether you’re using an API with your current CA or are interested in integrating one for the first time, GlobalSign specialists will work closely with you to ensure the integration functions exactly as you need.
Certificate Management System	Venafi’s Encryption Director Certificate Manager has a direct connector to GlobalSign’s certificates services.

CONCLUSION

Your managed SSL vendor should provide more than just certificates. Choose a company that offers cutting edge technology, flexibility to develop solutions to fit your needs, and the ability to advise on your organization's security concerns.

GlobalSign has helped dozens of organizations successfully make the CA switch, including the largest retailer in the US. Over 250 thousand domains are secured by GlobalSign and its customers span all verticals, including the second largest auto manufacturer in the US and the largest telecom company.

"The overall pricing, support, and flexibility of the system and the approach to certificate management are fantastic. Bottom line, GlobalSign is a refreshing, forward-thinking approach to SSL Certificate management. I would highly recommend giving them a serious look." [9]

Organizations that trust GlobalSign include known and trusted brands:

ABOUT GLOBALSIGN

GlobalSign has been a trust service provider since 1996. Its focus has been, and always will be, on providing convenient and highly productive PKI solutions for organizations of all sizes. Its core Digital Certificate solutions allow its thousands of authenticated customers to conduct SSL secured transactions, data transfer, distribution of tamper-proof code, and protection of online identities for secure email and access control. Vision and commitment to innovation led to GlobalSign being recognized by Frost & Sullivan for the 2011 Product Line Strategy Award. The company has local offices in the US, Europe and throughout Asia. For the latest news on GlobalSign visit www.globalsign.com or follow GlobalSign on Twitter (@globalsign).

CONTACT US OFFICE

One Broadway
Cambridge, MA 02142

1-877-775-4562
sales-us@globalsign.com
www.globalsign.com

[9] Brendan Hourihan, Director of Network and Desktop Support Services, Flagler College as quoted in https://www.globalsign.com/resources/case-study-flagler-college-mssl.pdf

REFERENCES

1 Gartner, X.509 Certificate Management: Avoiding Downtime and Brand Damage, Eric Ouellet & Vic Wheatman, 4 November 2011

2 Gartner, How to Succeed in Revamping Your PKI Program, Brian Lowans & Eric Ouellet, 4 May 2012

3 Gartner, Evaluating SSL Certificates for E-business, Vic Wheatman, 30 August 2011

4 GlobalSign CTO Ryan Hurst as quoted in Salvaging Digital Certificates, Paul Roberts, http://www.darkreading.com/security/application-security/240062664/salvaging-digital-certificates.html

5 Richard Stiennon, noted security author, speaker and founder of IT-Harvest as quoted in https://www.globalsign.com/company/press/111512-ssl-configuration-checker-provides-guidance.html

6 Matthew Prince, co-founder and CEO of CloudFlare as quoted in https://www.globalsign.com/company/press/110112-cloudflare-partnership-accelerates-secure-web-page-load-speed.html

7 Ivan Ristic, director of engineering at Qualys as quoted in https://www.globalsign.com/company/press/111512-ssl-configuration-checker-provides-guidance.html

8 Richard Sprigg, Dudley Metropolitan Borough Council as quoted in https://www.globalsign.com/resources/case-study-dudley-council.pdf

9 Brendan Hourihan, Director of Network and Desktop Support Services, Flagler College as quoted in https://www.globalsign.com/resources/case-study-flagler-college-mssl.pdf