# Cost and Security Benefits of SaaS-based Certificate Authorities

How Enterprises Benefit From SaaS Security and Management

## Introduction

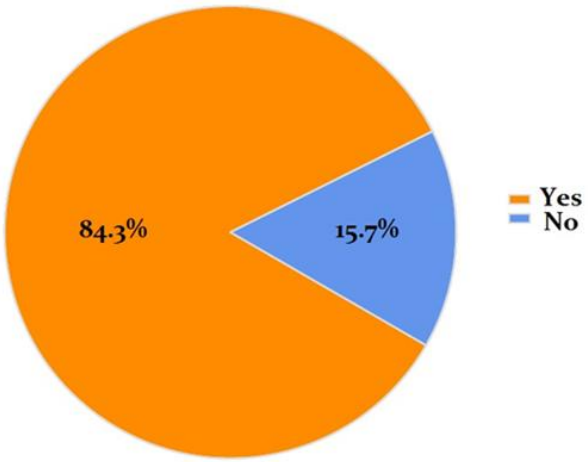
Digital certificates are an essential part of the foundation that enables secure digital communications, providing secure access to data, applications and cloud infrastructures. Digital certificates are an established, standards-based method to enhance trust over vulnerable networks. They are the digital equivalent of a driver's license or any other form of identity issued by a trusted third party in the physical world. Just as physical IDs ensure trust in the real world, digital certificates ensure trust across the Internet and within private networks, allowing parties to use digital identities to authenticate to each other and subsequently secure transactions and communications between their servers, systems, machines and users in enterprise and cloud environments.

Enterprises use two different types of certificates to secure their IT environments: those that are issued from an internal Certificate Authority (CA) such as Microsoft Certificate Services and those issued by public SaaS CAs. Internal CAs require the company itself to create, sign and manage certificates, a process that requires advanced knowledge of the complex Public Key Infrastructure (PKI) environment and significant time and human resources. The SaaS-based providers eliminate the management hassle internal CAs often cause by providing process automation, the latest in security technology, PKI service management, strong SLAs and technical expertise.

## Summary

GlobalSign, the enterprise SaaS-based CA, recently conducted a survey of enterprise IT professionals on the advantages of using a SaaS CA versus an internal CA such as Microsoft Certificate Services. It found that an overwhelming 84 percent of the professionals surveyed use digital certificates to secure applications accessed by internal and external digital identities, and that many of these companies utilize both internal and third-party certificates (See Figure 1). Another key finding was that 100 percent of respondents that use SaaS-based CAs feel that their SaaS CA allows them to meet their security and compliance standards and their policy guidelines, and that 47 percent of respondents are required to use SaaS CAs for their particular use-cases. The following are key findings of the survey and show how enterprises use CAs to ensure trusted communications.

**Figure 1: When asked if they use digital certificates to secure applications, 84 percent of the respondents said yes. .**



## Key Survey Findings

### *To Microsoft or Not to Microsoft*

Microsoft Certificate Services runs on a Windows server operating system and offers customers the ability to request certificates free of charge on an as-needed basis. The service also includes programmable interfaces for creating support for additional transports, policies, and certificate properties and formats. While the service is free, it requires technical expertise, maintenance and most importantly, significant IT resources.

GlobalSign asked survey respondents why they use the Microsoft service. An overwhelming 70 percent stated it is because the service is available at no charge. But as you will read further on, this is one of the few benefits Microsoft provides.

GlobalSign also asked respondents why they do not use Microsoft Certificate Services. Fifty-one percent noted that they face challenges in understanding the certificate template provided and that they do not have the required in-house PKI expertise needed. The additional findings below emphasize the toll that the administrative demands of implementing internal CA programs take on organizations.

- 45 percent responded that internal CA management is complex and noted that they would rather use a SaaS CA provider
- 50 percent responded that they do not have the adequate internal resources, staff or technical expertise needed to audit and manage digital certificates
- 65 percent are required to use public certificates because of their use-cases
- 53 percent do not want to bear the burden of maintaining the ever-changing PKI security best-practices required to operate an internal CA

### *Benefits of Public SaaS CAs*

There are many benefits to using SaaS CAs, especially as enterprises' use of the cloud and mobile technology grows at an exponential rate, resulting in an accelerated need for digital certificates. The GlobalSign survey found that 55 percent of the respondents utilize SaaS CAs to issue digital certificates that secure applications used to access data via their corporate network. Of those that use SaaS CAs, 47 percent use these third-party certificates to secure 50 percent to 100 percent of their applications.

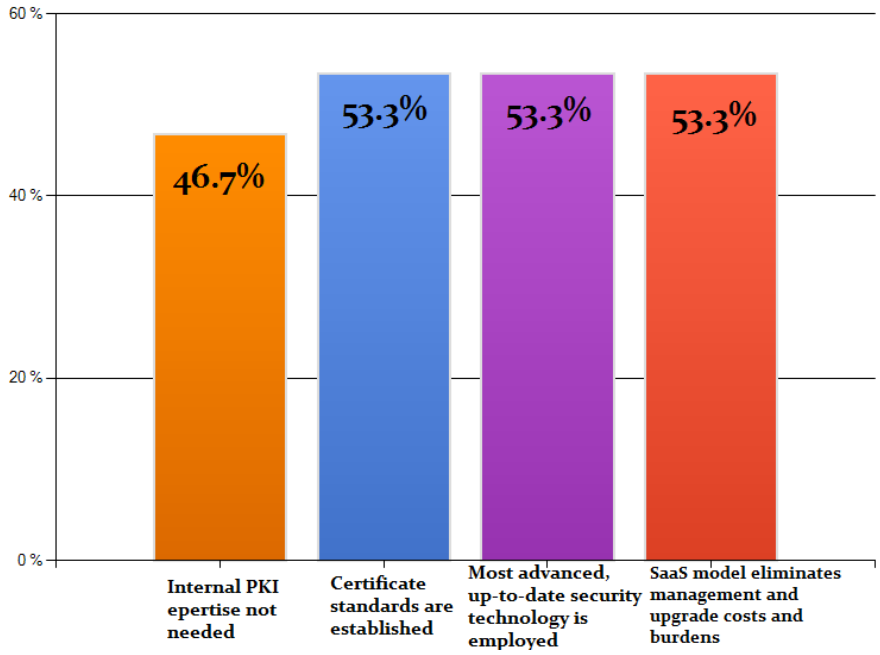
SaaS CAs provide relevant and updated policy, offer the most advanced technology and customer support, and are the strongest option in supporting trusted transactions inside and outside of private networks. In short, they provide the same functionality as the internal CA option without the administrative burden or the technical expertise, which that option needs. In fact, 44 percent of the survey respondents believe that compared to Microsoft Certificate Services it is much easier to utilize and manage the CA process with a third party.

The survey also showed that use of SaaS CAs will continue to grow, with 44 percent of IT administrators noting that they plan to increase use of SaaS-provided certificates. Over 25 percent of those that plan to increase use of SaaS certificates also plan to increase the percentage of SaaS certificates in their network

environments to over 50 percent. Below are other key findings that demonstrate in what ways respondents find SaaS CAs easier to use (See Figure 2):

- 47 percent of respondents say that SaaS CAs make certificate issuance easier because they do not require internal PKI expertise
- 53 percent say it is easier to use SaaS CAs because their certificate standards are already established
- 53 percent say SaaS CAs provide the most advanced, up-to-date security
- 53 percent of respondents say that the SaaS CA model eliminates management and upgrade costs and burdens

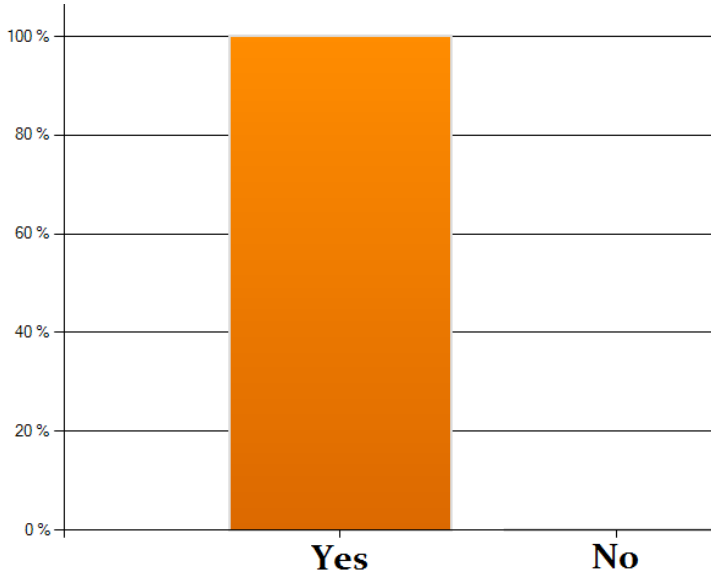
**Figure 2: In this multiple-choice question, respondents who answered revealed why they think it is easier to use a SaaS-based CA.**




***What About Security?***

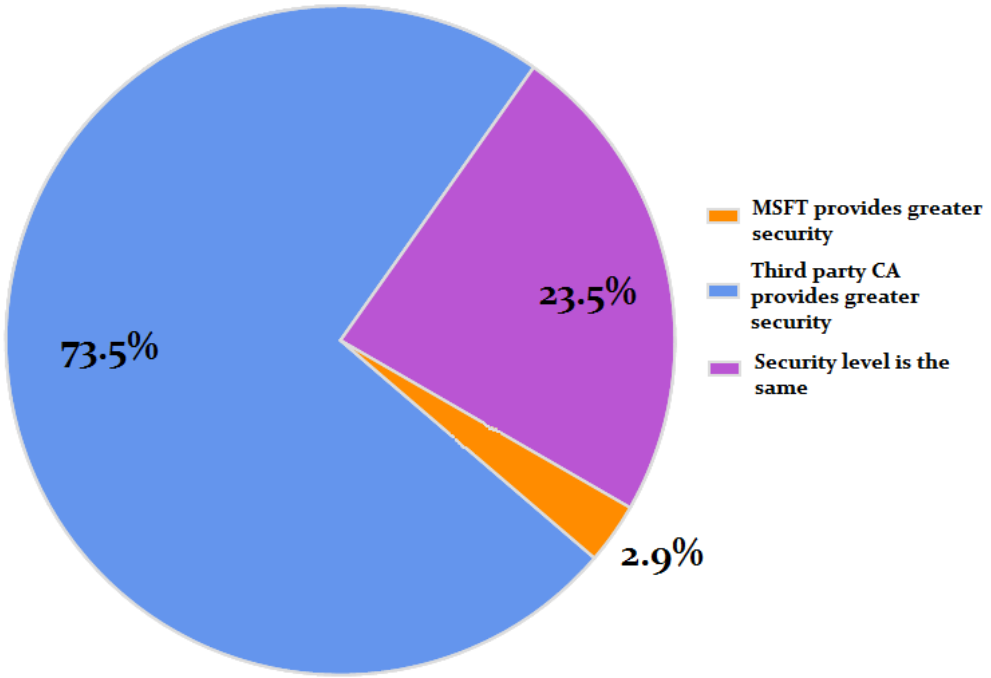
Certificates are the foundation of enterprise security; they provide enterprise networks the trusted signature that enables secure communications, allow private sharing of information and protect sensitive data. Pivotal to establishing the security of the certificate environment are the certificate policy and the Certificate Practice Statement, which defines the actors within a PKI environment and establishes their roles and duties. One hundred percent of survey respondents reported that their SaaS CA is able to help them meet their security and compliance standards policy guidelines (See Figure 3).

**Figure 3: When asked if their SaaS CA is able to help them meet policy guidelines, of the respondents who answered, 100 percent said yes.**




Possibly the most telling takeaway of the survey was revealed when respondents were asked which type of CA provides greater security. Seventy-four percent answered that SaaS CAs provide greater security, 3 percent answered that Microsoft Certificate Services provides greater security, and 24 percent believe the security level of both is the same (See Figure 4).

**Figure 4: When asked if Microsoft Certificate Services or their SaaS provider delivers greater security, of the respondents who answered, 74 percent said their SaaS providers do.**



## Conclusion

The enterprise demand for secure digital identities, trusted communications and protected transactions continues to grow at an exponential rate as businesses, workforces and customers have access to unlimited information, anywhere, at any time. With the emergence of iPv6 and the "Internet of Things," or "Internet of Everything" as GlobalSign likes to refer to it, the need for trusted communications will accelerate.

Secure access will not be possible without implementing a method of authentication that establishes trust between users and IP-identified objects. Digital certificates are a proven, scalable and secure method to implement high-assurance transactions over vulnerable networks. The world's constant connectivity has brought a new sense of urgency to enterprise IT professionals who are trying to meet the enterprise's security requirements and avoid interruption of mission-critical applications that rely on digital certificates for verifying identities. Outsourcing the operations of CA management, while retaining control on policy, helps customers focus on sales cycles and prevents unauthorized access to sensitive information and communications – or anything that can affect the company's bottom line.

SaaS CAs offer enterprises the most sensible solution for securing their information in this ever-connected world by providing the most up-to-date technology, established management and easy deployment of digital certificates.

## Methodology

The survey polled 154 respondents from various industries, including but not limited to financial services, healthcare, manufacturing, government, retail and technology. Titles of respondents include but are not limited to CEO, vice president, director, IT manager, network administrator and systems administrator. Not all questions applied to all respondents; percentages are based on the number of respondents who answered questions specific to each findings area.

## How GlobalSign Can Help

For more information on GlobalSign products and services visit www.globalsign.com.

To follow GlobalSign on Twitter, click here.

Interact with GlobalSign on Facebook, click here.

## About GMO 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).

**GMO Internet Group**

GMO Internet Group is a comprehensive provider of industry-leading Internet solutions including domain name registration, cloud-based and traditional hosting, ecommerce, security, and payment processing services that each hold the top share of their respective markets in Japan. Other key business areas for the Group include online securities/FX trading, Internet advertising, search engine marketing and online research, and smartphone game development and publishing. GMO Internet, Inc. (TSE: 9449) is headquartered in Tokyo, Japan. Please visit http://www.gmo.jp/en for more information.