DATASHEET

Certificate Lifecycle Management, Discovery & Provisioning

The Need for Better Digital Tracking

Digital certificates are the most secure and prevailing way of protecting identities and devices. As the number of people within organizations and connected devices increases, deploying individual certificates for each application can become a challenge for IT Teams. They have to stay on top of:

- Issuance, renewals and revocation to ensure business continuity
- IT operational costs
- Preventing downtime of business services

With IT departments handling a significant volume of digital certificates, they need management and monitoring tools to improve their operational efficiency and effectiveness.

Certificate Lifecycle Management is at the Core of Certificate Discovery and Provisioning

GlobalSign is one of the leading providers of trusted identity and security solutions for both internal and external facing PKI. Whatever your certificate lifecycle management needs, we can help. We offer managed services and on-premise solutions for Certificate Lifecycle Management and Provisioning as well as Certificate Discovery. We can fulfil the majority of PKI problems with our own proprietary solutions but also partner with leading technology vendors to deliver specialist services that are readily integrated with GlobalSign.

Three core benefits of using a Certificate Management Service (such as GlobalSign's Active Directory connected Auto Enrollment Gateway Service - AEG):

- **Know what you have through centralized management & reporting**
- **Delegate administration**
- **Save time and money**

KEY ADVANTAGES

- Find and monitor internal and public digital certificates from one location, regardless of issuing CA, including self-signed
- Save valuable time and resources over manual monitoring
- Eliminate server and application downtime due to certificate expiration
- Protect your brand by ensuring the availability of public-facing resources
- Avoid unexpected expiration with automated certificate renewals
- Easily track the source/issuing CA for all of your certificates
- Centralize your view of certificates that may have been purchased ad hoc by other individuals or departments
- Keep up with internet industry requirements and best practices with the ability to run reports on key length, hashing algorithms and other configuration options
- Reduce your organization's risk of non-compliance
- Ensure certificates are issued via your established processes and procedures
- Free up IT staff to focus on core competencies rather than tedious certificate management tasks

Common Authentication and Encryption Challenges

There are several main drivers for authentication and encryption, which can lead to bottlenecks and other challenges for IT teams tasked with managing their organization's digital certificates.

Risk Reduction

Cyber attacks have increased exponentially over the last decade, with many attacks exploiting vulnerabilities in unknown or untrusted digital certificates. These factors have left IT departments with the huge responsibility of tracking the location of every digital certificate deployed within their network. Do they know where they have digital certificates installed?

The answer is likely no but even if they do, it's difficult to manually compile all the information easily. Organizations often order certificates from multiple vendors and install them throughout their networks, both internally and in the cloud. While there are many advantages to this flexible, custom approach, it can be difficult for each department to effectively manage their certificates. The remedy to this is to use a Certificate Lifecycle Management tool.

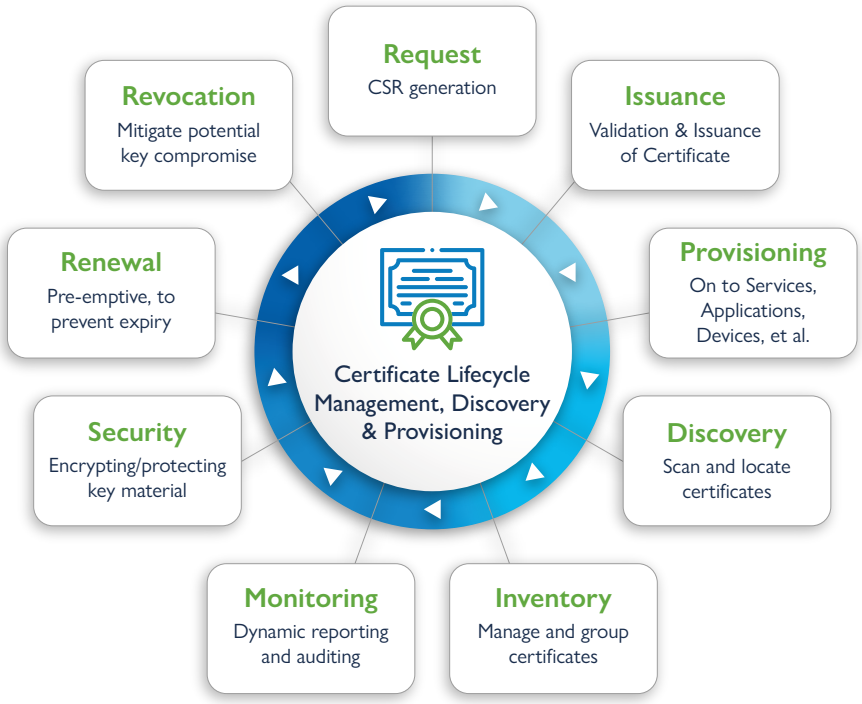
Compliance

Data Privacy and Data Protection is now one of the most critical priorities for organizations today. With data breaches at an all-time high and regulations such as the GDPR, PCI-DSS, HIPAA and NYDFS in force, organizations should be focusing on data security. Certificate based encryption is an effective technology solution that can enable organizations to meet and manage the compliance requirement easily with the use of Certificate Lifecycle Management tools.

Beyond risk and compliance factors, there are many other reasons why certificate lifecycle management plays a critical role in business operations.

Expired Certificates Cause Catastrophic Outages

Internally, expirations disrupt critical processes that are dependent on authentication and encrypted communication. There have been many industry examples over the past few months and years where expired certificates have cost well-known organizations hundreds of millions of dollars. As an example, In December 2018, the O2 mobile network shut down across the UK, impacting 32 million users and costing an estimated $100 million because of an unidentifiable expired SSL/TLS certificate. Furthermore, expired public SSL/TLS certificates can trigger alarming warnings in browsers, effectively taking your website offline. This could dramatically damage your company's reputation and leading to a natural loss of income and customer churn.



Unknown or Hidden Certificates Could Be Lurking in Your System

Does your company know what certificates are in your infrastructure? Certificate Discovery solutions help you locate digital certificates, including but not limited to SSL/TLS certificates. The results should be available in an easy-to-read format, allowing you to run reports on usage, upcoming renewals, configurations and CA issuance. It also allows you to identify the services that are not currently using certificates but should be.

Without Automation, Certificate Provisioning is Tedious and Time-Consuming

Installing certificates manually across more than just a handful of devices becomes painstaking and expensive. Just as it is imperative to be able to discover and manage digital certificates across your environment, being able to automatically install certificates onto servers and devices is equally important.

Certificate Management is Key to Business Continuity

"*By 2020, enterprises that use dedicated X.509 certificate management tools will suffer 70% fewer certificate-related issues and only half the time managing these issues as compared to enterprises using spreadsheet-based management methods.*" – Gartner

A managed service gives you the necessary tools to fully control your digital certificates. Whether certificates are used for encryption, identity or authentication, the use of these tools helps to offload some of the repetitive administrative tasks associated with certificate management.

Find out more by contacting us today – we will be glad to help you!

About GlobalSign

GlobalSign is the leading provider of trusted identity and security solutions enabling businesses, large enterprises, cloud service providers and IoT innovators around the world to secure online communications, manage millions of verified digital identities and automate authentication and encryption. Its high-scale Public Key Infrastructure (PKI) and identity solutions support the billions of services, devices, people and things comprising the Internet of Everything (IoE).

US: +1 877 775 4562
UK: +44 1622 766766
EU: +32 16 89 19 00

sales@globalsign.com
www.globalsign.com

GlobalSign®
GMO INTERNET GROUP