Keyfactor helps GRENKE streamline certificate management in the face of rapid growth

GRENKE

Industry

Financial Services

Location

Baden-Baden, Germany

Pain Points

Too many different certificate authorities and templates

Disruptive service outages caused by expired certificates

No time for IT to plan and implement longer-term objectives

Solution

Keyfactor Command

Company Overview

The GRENKE Group is a global financing partner for small and medium-sized companies. As a one-stop shop for customers, GRENKE's products range from flexible small-ticket leasing to demand-driven bank products. Fast and easy processing and personal contact with customers and partners are at the centre of GRENKE's activities. Founded in 1978 in Baden-Baden, the Group operates in more than 30 countries and employs approximately 2,100 staff (measured in terms of full-time equivalents) worldwide.

Challenges

At the dawn of the computer revolution, in 1978, GRENKE was founded in Baden-Baden, Germany. The idea: To enable small and medium-sized businesses to lease office equipment starting with a volume of as little as 500 euros (small-ticket leasing).

As the company grew and information technology evolved, it expanded the range of equipment that companies could finance through leasing. Today, GRENKE offers a broad portfolio of assets ranging from IT to medical equipment to green economy objects such as wallboxes, photovoltaic systems and e-bikes – and has become a global company, operating in more than 30 countries worldwide.

Growing alongside the IT industry through the globalization of business meant that the company had to adopt new standards and

technologies as they emerged, including the use of PKI. As a result, GRENKE found itself with an increasingly unmanageable hodge-podge of PKI solutions and methods for issuing certificates to keep its IT systems running.

"It was quite chaotic," said Olaf Rohleder, Systems Engineer for GRENKE, who was given oversight for the company's PKI and certificate management in early 2020. "We had 3 different PKI systems and about 70 different certificate templates. At that time, we experienced roughly 60 outages, because unknown or untracked certificates would expire, and we wouldn't know about it until systems went down."

The need was urgent. For internal certificates, Rohleder had to use the Microsoft Management Console for certificate management, request the certificate, export it as a PFX file, then send it to the appropriate person. "For certificates from a public CA, CSRs [certificate signing requests] were created the same way, but then were uploaded to a certificate vendor to finally receive the certificate," he said.

It was a very manual process, requiring at least 30 to 45 minutes per public certificate, and he had 10 to 15 per week to handle. Meanwhile, the company suffered about 60 outages of some services in his first year on the job because of expired certificates.

Results

Reduced certificate-related task workload by at least 4 to 5 hours per week

Eliminated outages caused by expired certificates

Trained 60 individuals to handle their own certificate needs

Consolidated and streamlined PKI to just one internal PKI and one public CA

Products

Keyfactor Command

Solution

GRENKE selected Keyfactor to provide the solution for its certificate management headaches. Rohleder's first step was to identify all the certificates and get them assigned to teams for each of the company's lines of business. The next step was to replace GRENKE's outdated online root CAs. "I moved pretty quickly to kill and remove the Microsoft 2008 R2 CA. But the 2012 CA was our main PKI CA. We saw the certificate was only valid for another 18 months or so, and I said, 'No, I won't renew that certificate. I will put in a new, clean CA infrastructure.'"

Rohleder and his team put in a new offline root CA and two issuing CAs. All the automatically issued certificates, such as computers, remote desktops, and Windows Remote Management, are issued by a single CA. "Those we manage, such as web service certificates or code signing certificates," he said. "We issue those certificates

"[Now the users] do a lot of the work themselves, and I have more time to create new possibilities for them, including Linux servers. Over a year ago, I wouldn't have been able to do that, even if I had the technical capability because there still wasn't just enough time to test things out."

from our managed issuing CA, which we access with Keyfactor [and] enable our people to get certificates."

Now the company has a number of self-programmed applications that use different services, each requiring a certificate. There are code-signing certificates for some of the developers and administrators, which Rohleder's team can generate.

Now about 60 people are trained to use Keyfactor. They all have access to self-service, with the required permissions. Rohleder still provides some assistance because there are teams that only issue certificates once or twice a year, "but in principle, every user can now get themselves a web service certificate if they need one. And if the server where it is to be deployed is already added to Keyfactor, they can also automatically deploy it. It's helped our teams move at least 50% faster." As a result, the average time for an internal certificate is usually less than five minutes, just a little higher for a public certificate, he said.

"I can now get more proactive. I've actually had the time to develop a roadmap of what I want to do next."

Business Impact

Consolidated management of over 25,000 active certificates and positioned company for further expansion

The company has over 25,000 active certificates. Now, application owners can self-service their own certificates, and it only takes 5 minutes of work to configure it. Also, the company is poised for unlimited expansion as it continues to grow its financial services sector. Whereas before, it was having trouble managing the certificates that it had, it can now easily keep track of the old certificate pool and have the bandwidth for unlimited expansion.

Eliminated outages through automation

In the first year that Rohleder was in charge of straightening out the company's PKI and CA infrastructure, the company suffered 60 outages. Once the company committed to Keyfactor's solution, there were only three outages – and those were due to human error and overlooked certificates. Since those were corrected, there hasn't been a single outage. Through a combination of expiration alerts, automated renewal processes, and training of IT staff in the different business units, human error has been effectively eliminated from the equation.

"With Windows Servers, which is the mass of our machines, usually, I can fire and forget. As long as there is no technical problem with some firewall or whatever happens, it's usually within a quarter of an hour that it's on the server."

Improved productivity with self-service workflows

Rohleder has emphasized training to eliminate personnel bottlenecks. The training was quite straightforward, especially since most of the certificates work the same way – leaving him time to address the CAs that require more attention.

“We’re not completely automated, but from the beginning worked with Keyfactor as a self-service tool,” Rohleder said. “Now our application owners all have the access to Keyfactor with the permissions they need. They handle their certificate enrollments without intervention.”

About Keyfactor

Keyfactor brings digital trust to the hyper-connected world with identity-first security for every machine and human.

Contact Us

- www.keyfactor.com
- +1.216.785.2990