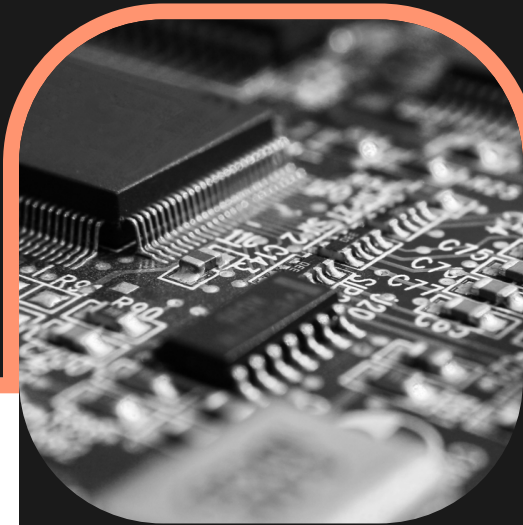# Global Manufacturer Automates PKI & Strengthens Security-Developer Alignment with Keyfactor

Company Overview

This global manufacturer is one of the world's leading suppliers of sensing, electrical protection, control and power management solutions, with operations and business centers in 12 countries. Their products improve safety, efficiency and comfort for millions of people every day in automotive, appliance, aircraft, industrial, military, heavy vehicle, heating, air-conditioning and ventilation, data, telecommunications, recreational vehicle and marine applications.

Challenges

As a publicly traded international organization, this customer prioritizes the security across all of its solutions. Several years ago, this led them to introduce Keyfactor Command to help manage its public key infrastructure (PKI).

However, the global manufacturer was barely scratching the surface of what was possible with all of Keyfactor, according to Rich Popson, Senior Information Security Manager, who is responsible for information security, cyber risk and privacy for the organization.

Industry

Electrical & Electronic Manufacturing

Company Size

Global 2000

Empoyees

22,000+

Keyfactor Products

Keyfactor Command
Keyfactor Signing Solution

Certificates Managed

72,000+ Total
18,000+ Active

Specifically, Popson and his team identified several additional use cases for Keyfactor to solve challenges around:

- Efficiently managing the full certificate lifecycle for over 72,000 certificates

- Lowering the cost of issuing certificates

- Introducing a "trust but verify" environment, especially for a remote workforce

- Leading SSL scanning activities

- Empowering developers to move at the necessary speed while maintaining security

- Tightening security of private keys for code signing to ensure proper protection of client data

"I've been around long enough to see how difficult certificates and PKI environments are to maintain and secure, and there's no way we would be able to properly maintain the security for all those certificates without this type of solution. It's just easier with Keyfactor,"

Solution

Over the past year, Popson and his team have made the business case internally for renewing and growing their relationship with Keyfactor to satisfy these new use cases. In doing so, they've pinpointed three critical solutions Keyfactor has delivered:

1. Readily scalable certificate lifecycle management

2. Improved security for a growing mobile workforce

3. Enhanced speed and protection for developers

Readily Scalable Certificate Lifecycle Management

First, this company has continued to use Keyfactor Command to introduce scalable certificate lifecycle management for the organization's PKI. This scalability allows Popson's small team to efficiently monitor and manage over 72,000 certificates across the entire organization.

For example, Popson uses Keyfactor to generate reports that provide immediate access to information like the number of:

- Total certificates the organization has issued

- Active certificates

- New certificates issued each week

- Self-signed certificates

- Certificates expiring in one week, two weeks, two months and six months

The team can also set up expiration alerts through Keyfactor and introduce rules for auto-renewal of expiring certificates.

According to Popson, this type of automation and easy access to certificate information is a game-changer. "I've been around long enough to see how difficult certificates and PKI environments are to maintain and secure, and there's no way we would be able to properly maintain the security for all those certificates without this type of solution. It's just easier with Keyfactor," he explains.

In addition to the ease of scaling via automation, Keyfactor has also made it possible for the manufacturer to scale its PKI cost efficiently, since the team can use Keyfactor to issue their own certificates rather than having to purchase tens of thousands of certificates at $200-500 each from an external Certificate Authority (CA).

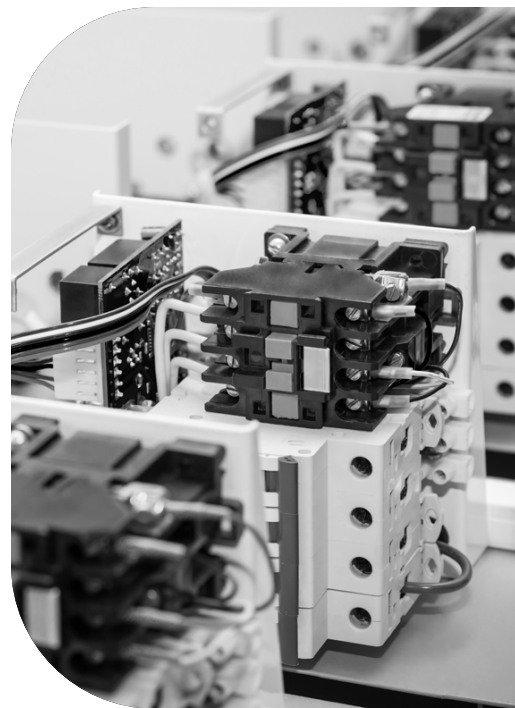## Improved Security for a Growing Mobile Workforce

The level of scalability Keyfactor has made possible has become particularly important to securing a growing mobile workforce. Most recently, this has come into play as the COVID-19 pandemic forced an overnight shift to near 100% remote work.

"The cloud-hosted PKI made possible by Keyfactor has been essential during COVID-19. We now need to offer security solutions for more remote workers and we have to enable our developers to sign code remotely — all while the entire security team is remote too. This situation has made the web-based nature of Keyfactor Command even more critical for our team," Popson says.

Along the same lines, Keyfactor has allowed this company to move towards a "trust but verify" approach. As Popson describes it: "Keyfactor has helped us move away from the brick-and-mortar firewall approach to security. Now we can trust but verify, so we can protect devices that are outside the firewall or even allow employees to use personal devices like smartphones. Keyfactor has made this possible because we can only trust a device if we can verify it, and the only way to do that is with certificates."

Enhanced Speed and Protection for Developers

Next, Keyfactor has enabled the customer's security team to create faster processes for their developers. Previously, as developers spun up and brought down new servers during the development

process, they would often run into roadblocks created by expired certificates. Upon identifying this challenge, Popson's team offered a solution in the form of self-service certificate issuance through Keyfactor.

This solution proved to be a big win, as it helped avoid costly slow-downs for developers and paved the way for additional conversations between the two teams. Popson says his team has put in a lot of work recently to further bridge the gap between security and development processes by forming committees to understand different procedures and responsibilities and by acting as internal consultants on security requirements for new projects.

The customer has made great strides in this regard, identifying development challenges around SSL scanning and secure code signing with which the security team was able to help through the use of Keyfactor. For example, they found opportunities to tighten security in how developers store private keys for code signing that can reduce risk for the organization and end up saving millions of dollars as a result. The security team quickly determined that Keyfactor's signing solution would provide a cost-effective solution to this challenge and successfully made the business case to implement the additional Keyfactor product.

Now, with Keyfactor's signing solution in place, instead of sharing private keys over channels like email, clients can create a login, upload their private key to give the customer's developers the necessary access and then easily monitor who's using it and how. Importantly, they can also revoke access at any time.

The Results

This customer has realized numerous benefits since introducing and later expanding their relationship with Keyfactor. Specifically, working with Keyfactor has resulted in:

Significant time and cost savings for the customer's security team:

The fact that Keyfactor is cloud-hosted and offers automated certificate lifecycle management allows the security team to focus on getting work done rather than maintaining the system.

> "Keyfactor just works. And when we do need support, the Keyfactor team is always willing to help right away without nickel and diming us."

Competitive advantage from reduced risk in handling client data:

The ability to properly obtain and secure private keys for code signing with Keyfactor's signing solution and introduce automated SSL scanning with Keyfactor Command have increased security for critical data and improved protection against certificate failures. As a result, these improvements help avoid detrimental outages that could result in fines, increase trust among clients and provide a competitive advantage for growing revenue and protecting against client churn.

Better alignment between the customer's security and development teams:

Keyfactor has allowed the customer's security team to better meet developer needs around speed of delivery, for example by allowing developers to obtain certificates on demand via a self-service process and by introducing a directory of trusted programs on developer devices — all without sacrificing security. These initial advancements have opened the door for more conversations between the security and development teams, who are now working closely to introduce new processes to further improve alignment.

Along the way, Popson notes that the Keyfactor team has been critical to the customer's success. "Keyfactor just works. And when we do need support, the Keyfactor team is always willing to help right away without nickel and diming us," he says. Popson adds that Keyfactor has even gone beyond to offer presentations on PKI for groups within his company who are interested in learning more, which in turn has helped Popson gain buy-in to continue growing the program.

Going forward, Popson shares that PKI will become even more essential to his team's work, and he plans to continue to grow the relationship with Keyfactor to make that happen. Says Popson: "We continue to make advancements in our IoT products which carry a lot of data. There's a lot of risk there that we need to make sure we protect against, and certificates are the best way to do so. From a strategic standpoint, it just makes sense to work with Keyfactor on that because Keyfactor allows us to keep everything in one portal and enables us to be our own CA for our own devices, saving us significant time and money."