Phoenix Contact Secures IoT Devices with Modern PKI Platform

Company Overview

Phoenix Contact is a global leader in automation technology, developing innovative solutions in connection technology, electronics, and automation for over 100 years. Headquartered in Germany, the company serves diverse sectors, including industrial production, renewable energy, and infrastructure.

Challenges

Compliance in automation manufacturing is tough, especially when it comes to securing IoT devices. Regulations are constantly changing. But Phoenix Contact saw an opportunity where others saw a challenge. By rethinking their approach to Public Key Infrastructure (PKI), they transformed their entire operation.

“Cybersecurity is a very difficult thing to do, and until recently, nobody really paid too close attention to cybersecurity for devices on the shop floor. Now, that’s all changing thanks to the increasing threat landscape and new European regulations,” explains Lutz Jänicke, Corporate Product & Solution Security Officer at Phoenix Contact. This was an opportunity to strengthen their security posture and protect their customers.

Industry

Automation Machinery Manufacturing

Location

Blomberg, Germany

Pain Points

Increasing cybersecurity for IoT devices

Maintaining compliance with new EU regulations

Managing secure device identities and signing certificates

Solution

Phoenix Contact leverages Keyfactor EJBCA to automate secure identities for IoT devices, simplify certificate management across diverse use cases, and modernize PKI with a unified approach to meet stringent regulatory and compliance requirements.

Two recent regulations, in particular, have forced a new level of scrutiny around cybersecurity among European companies like Phoenix Contact. The first, NIS 2, targets operators by introducing security standards within companies and on the shop floor itself, while the second, CRA, focuses on consumer and industrial products and the level of protection offered within them.

In response, Phoenix Contact is strengthening cybersecurity management for its operations and building secure processes for device identities as part of IoT product development. Many of these processes already exist throughout different areas of the company, but they now need to be extended end-to-end across the entire company and product portfolio.

"One of the most important things is the integrity of our products. So we need to ensure that all of our software and firmware is correctly signed, which requires a strong PKI program to manage those signatures and certificates. At the same time, we want to enable our customers to verify whether they buy genuine Phoenix Contact products. That means we also need to support secure device identities," Jänicke shares.

Specifically, Jänicke cites IEC 62443, a standard for industrial automation that requires the use of secure digital signatures and secure digital identities. He notes that the Phoenix Contact security team is currently working to make sure they can fully meet that standard across all of their processes. Meeting this standard was a significant milestone on Phoenix Contact's path to compliance excellence.

Solution

The Phoenix Contact team knew they would need a PKI solution to help meet their compliance goals in a standardized and streamlined way. Market research on potential solutions led Jänicke to Keyfactor EJBCA.

"I immediately liked that Keyfactor had a community edition product that allowed us to evaluate it without a lot of discussion and see the quality of the offering for ourselves. And after using that product and comparing it with other offerings, we chose to work with Keyfactor long term," he says.

Results

Standardized and streamlined management for signature certificates

Improved ability to support a variety of digital signature requirements

Increased security through device identity management

Clear roadmap for phasing out Microsoft ADCS

Support from a team of PKI experts

Products

Keyfactor EJBCA

"Keyfactor is stable and mature. And in this market where PKI has to operate for years or even decades, it's important to have a partner with staying power. So far, working with Keyfactor has delivered that strength."

Lutz Jänicke,

Corporate Product & Solution Security Officer
Phoenix Contact

Jänicke notes that one of the biggest selling points for Keyfactor was the flexibility it offered, with options for PKI as a Service and more. With Keyfactor, Phoenix Contact found a partner who could help them cut through the complexity and take control of their PKI.

Additionally, Keyfactor checked all the boxes for Phoenix Contact's requirements, including a fully automated process for issuing device identities and supporting secure digital signatures across a variety of use cases.

On the flip side, Jänicke shares that most of the other offerings the team evaluated were not as robust as Keyfactor and required more manual processes, which made it difficult to verify the quality of those solutions overall.

"Operating PKI requires certain skills, knowledge, and manpower that Keyfactor has proven they can deliver on."

Business Impact

After more than four years of working with Keyfactor, Phoenix Contact has successfully standardized and streamlined cybersecurity across the organization. Specifically, Jänicke cites three key areas of impact since working on introducing Keyfactor EJBCA:

Ability to evolve alongside use cases

Phoenix Contact has a variety of use cases, and this requires the security team to support numerous different types of signatures. Although Jänicke found that Keyfactor did not natively support all of these use cases, he was able to work with the Keyfactor team to develop additional signature formats as needed. This flexibility and responsiveness proved valuable in ensuring Keyfactor could work for all of the company's ongoing needs.

Building on this, Jänicke notes that he continues to find new ways to use Keyfactor for different PKI needs. He explains: "We are currently evaluating how we can expand our use of Keyfactor for device identity management, as the approach we're taking to secure our products is evolving all the time. Additionally, we are looking at how we can use a product like Keyfactor Command to improve our certificate lifecycle management."

"The PKI program under Keyfactor has become the stable core, with policies for our administration and operational concept, so we are considering rolling that out across the rest of our PKI services."

Lutz Jänicke,

Corporate Product & Solution Security Officer
Phoenix Contact

Single source of truth for device identities and certificate management

Currently, Phoenix Contact uses Keyfactor EJBCA for two main purposes:

1. **Providing a digital identity to all relevant devices:** Whenever a device is produced, the digital identity is programmed in through Keyfactor. This is a highly automated process based on one certificate hierarchy in EJBCA.

2. **Managing all of the signature certificates:** Tracking all of the certificates used for signing, for example signing firmware or signing Secure Boot applications, happens through Keyfactor. This process relies on a second certificate hierarchy within EJBCA.

These two use cases alone offered a notable improvement for identifying and managing device IDs and certificates, but Phoenix Contact has even more planned. According to Jänicke, his team is currently working on a project to bring all enterprise PKI efforts together. A big part of this effort is upgrading the remainder of Phoenix Contact's PKI services, many of which fall under the company's legacy program run by Microsoft Active Directory Certificate Services.

"When we first started this project in our IT department, we were using Microsoft ADCS, but it was just there without much of a team behind it. Now, the company has evolved. We have new people with new expertise, and we're looking to integrate all of our PKI efforts. The PKI program under Keyfactor has become the stable core, with policies for our administration and operational concept, so we are considering rolling that out across the rest of our PKI services," Jänicke says.

Support from a strong, stable partner

Overall, Jänicke reports he is very happy with EJBCA specifically and Keyfactor more generally.

"Keyfactor is stable and mature. And in this market where PKI has to operate for years or even decades, it's important to have a partner with staying power. So far, working with Keyfactor has delivered that strength," Jänicke shares.

Phoenix Contact has also found value in the overall expertise of the Keyfactor team, and Jänicke recommends others consider the value in that knowledge. He concludes: "Operating PKI requires certain skills, knowledge, and manpower that Keyfactor has proven they can deliver on. I would recommend other organizations to consider whether they can manage a PKI program themselves or whether they should rather focus on a managed service offering, like Keyfactor's PKI as a Service, to achieve their goals."

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
- +1.216.785.2946