Case Study

How Siemens AG Automated PKI Deployment and Achieved Zero Trust with EJBCA Enterprise

Company Overview

Siemens AG is a technology company focused on industry, infrastructure, transport, and healthcare. From more resource-efficient factories, resilient supply chains, and smarter buildings and grids, to cleaner and more comfortable transportation as well as advanced healthcare, the company creates technology with purpose adding real value for customers. By combining the real and the digital worlds, Siemens empowers its customers to transform their industries and markets, helping them to transform the everyday for billions of people.

For Siemens AG, trust is everything. Public key infrastructure (PKI) is an essential building block to establishing cryptographical trust across a growing number of its products and enabling an enterprise-wide zero-trust policy. For these reasons, Siemens operates an in-house PKI with Keyfactor EJBCA Enterprise. Due to high efficiency demands, managing manual deployment methods were less and less feasible. By adopting Red Hat Ansible, Siemens automated its entire PKI deployment to reduce time and production cost. Rufus Buschart, head of PKI at Siemens, led the team that oversaw the deployment of the required PKI for each use case across the organization.

Industry

Industrial Manufacturing

Location

Munich, Germany

Products

Keyfactor EJBCA Enterprise

Pain Points

Manual methods for deploying PKI infrastructure were infeasible

Scaling PKI to support a growing number of products and zero-trust strategy

Solution

Siemens AG leverages Red Hat Ansible and Keyfactor EJBCA to automate its entire PKI deployment, reducing time to market and production costs.

Benefits of a fully automated PKI deployment

While organizations can manage PKI deployments manually, doing so is time-consuming and laborious — particularly for large size deployments like Siemens'. Automating these processes saved Buschart's team time and allowed them to focus on other priorities. He noted that they were able to reduce time spent on the setup and deployment of a system from more than a week to just one day.

The setup process was automated using the Red Hat Ansible Automation Platform, which enabled Buschart's team to develop playbooks for the installation, configuration, hardening, and deployment of PKI operations at scale. Buschart explained that relying on the playbooks resulted in significant time savings for his team. He shared the example of setting up a database machine: when completed manually, the workflow required nine detailed steps that the team must execute very carefully. Now, all they must do is run the playbook.

To streamline PKI installations across most parts of the business, Siemens deployed EJBCA Enterprise — an end-to-end certificate management solution that also enables simplified and automated PKI operations at scale. In this use case, the playbooks do not just deploy EJBCA on a machine or in a lab. The entire process is automated, including the installation and hardening of Jboss according to the Siemens guidelines, and the configuration of the Hardware Security Module (HSM).

Automating PKI system deployment enables organizations like Siemens to be more agile when experimenting with new use cases. Compared to manual processes, less time is lost in an automated deployment if something does not work as planned. Thanks to the ease and speed of automated deployment, PKI teams like Buschart's can fail fast and readjust without wasting time and resources.

Organizations with similar infrastructure to Siemens can leverage these PKI deployment playbooks on Keyfactor's GitHub. Keyfactor released them as open source in production quality, so anyone with an understanding of EJBCA, Ansible, and their organization's PKI requirements can benefit from them.

> "Sometimes it was difficult to get things working right away or to deploy it on EJBCA. But every time we had an issue, Keyfactor and Red Hat helped us to solve it. It was a very productive relationship."
>
> **Rufus Buschart**
>
> Head of PKI, Siemens

Consistent results with PKI as code

Faster deployment is a major advantage of installing PKI as code, but it's not the only one. Turning previously manually conducted workflows into coded processes means the possibility of overlooking critical details within the process is removed from the equation. Regardless of how often a workflow happens, the results are always the same and the operation becomes easily repeatable.

Another advantage of this approach is having automated documentation. With Siemens' previous PKI solution, one challenge was that when someone left the team, their work may not have been documented properly. Some configurations had to be redone many times, costing the PKI team valuable time. In Siemens' current automated setup, the code itself is the documentation. If something changes, it's visible there.

Constant improvements along the way

Siemens' PKI team worked closely with Keyfactor and Red Hat Professional Services to enable its modern, highly scalable PKI. "Sometimes it was difficult to get things working right away or to deploy it on EJBCA. But every time we had an issue, Keyfactor and Red Hat helped us to solve it. It was a very productive relationship," said Buschart.

For Siemens, this was an enriching improvement process. Code was written and reviewed, and at times, the PKI team made further refinements to it. For example, they found that some tasks could be grouped, so instead of using several scripts, one script sufficed to consolidate them. Making these adjustments along the way benefited from automation as well. The "fail fast and readjust" approach enabled Siemens' administrators to incorporate improvements without losing unnecessary time.

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