SECTIGO

PKI for DevOps

Sectigo PKI Enterprise Use Case: DevOps

More and more companies are adopting DevOps to shrink development cycles and improve the quality and functionality of their products. But the DevOps environment introduces new challenges, particularly when it comes to ensuring security and identity processes. Today's DevOps teams don't want to spend their time on certificate management, and yet they need to:

- Integrate PKI to protect containers and the code within them
- Leverage public SSL certificates for load balancers and web server setup automatically using DevOps tools
- Issue, revoke, and replace certificates quickly, reliably, and scalably
- See and control the entire certificate lifecycle through a single user interface

Fortunately, Sectigo can help. Our Private PKI solution featuring Sectigo Certificate Manager provides greater automation and discovery of certificates at enterprise scale, while Sectigo SSL certificates allow for the automated provisioning of web server and load balancer certificates from the same pane of glass. And by centralizing and automating certificate issuance and management, it's easier to diagnose problems and prevent outages related to certificate deployment. With Sectigo, your DevOps team can incorporate compliant certificate processes into their normal workflow and start taking full advantage of:

- **Code Signing.** Sectigo Code Signing certificates allow developers to digitally sign applications and software programs, thereby verifying file sources and ensuring that their code has not been altered in any way. Using certificates, you can be confident that your deployed code is from a trusted source and is exactly what you intend it to be. Sectigo Code Signing supports all file types, including drivers, firmware, scripts, and applications. And Sectigo Certificate Manager automates and eases the entire certificate lifecycle, from issuance to renewal.

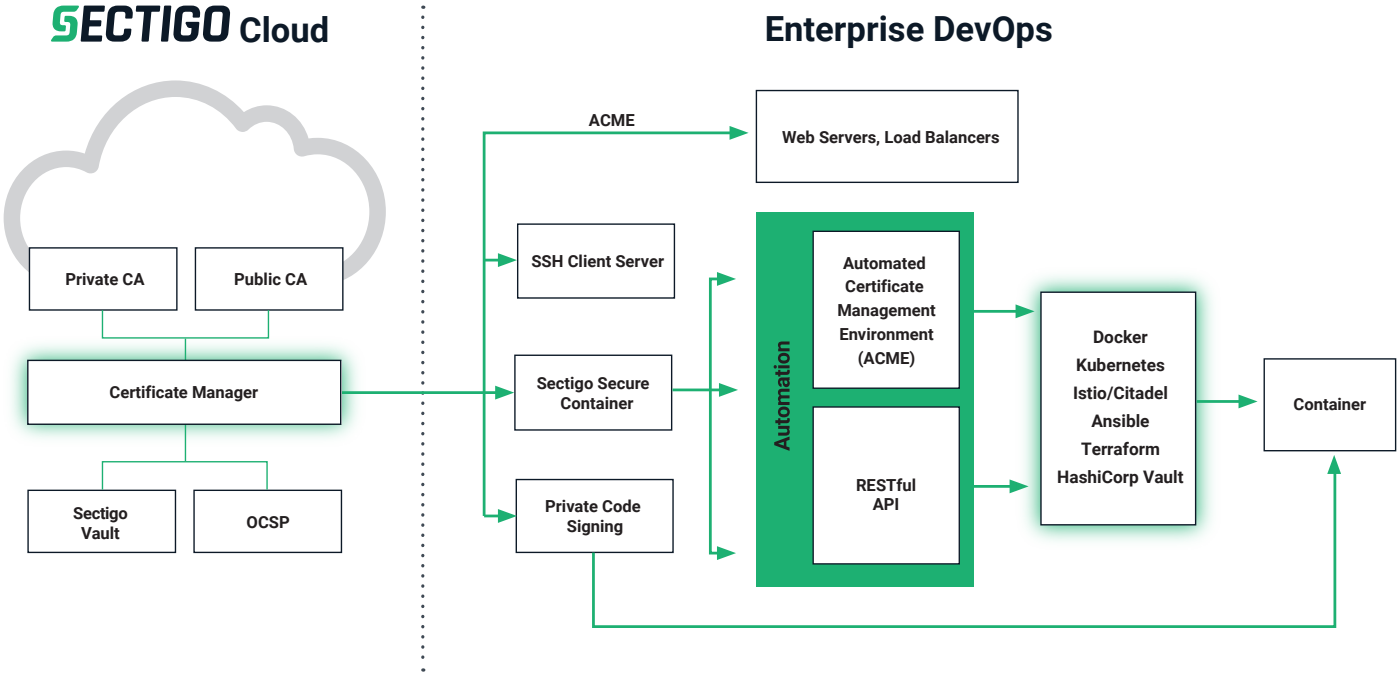
- **REST API for container certifications.** In DevOps environments, each container is provisioned a certificate to ensure that all containers in that system are authorized to connect to one another. With Sectigo Private PKI, you can quickly, easily, and automatically provision certificates for all your containers and associated tools. Through its RESTful API, Sectigo Certificate Manager can interoperate with a wide variety of DevOps development tools and environments.

- **ACME for SSL.** The Automation Certificate Management Environment (ACME) eases your certificate management burden and is supported by over 150 million web sites and more than 130 open source tools. Sectigo Certificate Manager can be used with a wide variety of DevOps environments such as Kubernetes, Chef, Ansible, Salt Stack, Terraform, Puppet, Istio, and Docker, all of which support ACME natively to easily and scalably secure your public-facing servers.

- **DevOps integrations.** Criteria include mechanisms to incorporate PKI into the continuous integration and continuous deployment (CI/CD) pipeline, orchestration frameworks (Docker Swarm), and third-party key vaults (HashiCorp's Vault).

Sectigo offers a variety of deployment options, as well as the convenience and security of a seamless solution with one pane of glass for both public and private certificate issuance and management. Moreover, with Sectigo, you will never run into a certificate volume cap, as you might with open source alternatives. With Sectigo Private PKI, SSL, and Code Signing certificates, your security team can easily enforce cryptographic security policy across your entire DevOps implementation, enable secure container communication, and protect and future-proof your applications.

DevOps PKI architecture



About Sectigo

Sectigo provides purpose-built, automated PKI solutions that secure websites, connected devices, applications, and digital identities. As the largest commercial Certificate Authority trusted by enterprises globally for more than 20 years, and more than 100 million SSL certificates issued in over 200 countries, Sectigo has the proven performance and experience to meet the growing needs of securing today's digital landscape. For more information, visit **www.sectigo.com.**

