Accelerate DevOps with Streamlined PKI
Since it was first introduced, the DevOps approach to software development has been synonymous with agility. DevOps drives flexible, lean operations by enabling direct collaboration across development and operations teams. It also has other benefits: increased automation, streamlined operational support, and happier customers are all made possible with DevOps methodologies.

According to current research, the DevOps market will grow to nearly $13 billion by 2025, driven by the adoption of IT automation and cloud migration. To support this enormous growth in these dynamic environments and compete in our information-rich and agile business world, developers, operations, and security teams must be able to collaborate in real time to meet the evolving demands of the market while also keeping their businesses safe.

In recent years, DevOps has gone from being novel to mainstream. In fact, Forrester Research declared 2018 “the year of enterprise DevOps.” According to Forrester, more than 50% of companies surveyed use internal or external DevOps services, in industries ranging from financial services and healthcare to e-commerce. Industry authorities at Gartner also include DevOps as a central approach for delivering “Fast IT,” with more than 75% of companies utilizing it. Unfortunately, the rapid, broad adoption of DevOps is leaving another crucial area neglected: security.

In most organizations, DevOps is a grassroots effort, with developers embracing DevOps practices and tools with little coordination across other teams. This results in the development of new applications that are not integrated into the organization’s security processes, causing applications to ship with security risks or vulnerabilities. But why has this become so common? Driven by the need for speed, developers often prioritize service-level agreement delivery times over what they may consider non-critical security requirements. Nevertheless, with the growth in machines and the increasing reliance on DevOps, incorporating proper security controls is essential.
Identity as the New Perimeter: DevOps and Machine Identities

Organizations worldwide are continuing to add more machines into corporate environments to keep pace with the growing digital universe. By leveraging machines and applications, companies can dramatically boost efficiency, increase speed, and drive agility. In the pursuit of these benefits, the explosive growth of machines has been dramatic and unprecedented.

Cisco’s Visual Networking Index recently revealed that machine deployments are increasing at a CAGR of 10% – a 7% higher growth rate than that of users accessing the internet. Additionally, the report notes connections between devices and applications will hit nearly 14 billion by 2021. This means the number of IP-connected machines will exceed the expected human population by 3x.

Although the number of machines is outpacing the number of people, and despite the fact that these machines are responsible for critical business functions and data, they often aren’t protected with the same scrutiny as people. Just as people’s identities are secured with usernames and passwords, each machine – whether physical or virtual – also requires its own unique identifier.

One of the keys to protecting applications is the use of SSL/TLS certificates that serve as machine identities for secure authentication and machine-to-machine communication. Certificates are used with everything from physical servers and laptops to virtual machines, containers, IoT devices, and mobile applications. As these machines are in a constant state of real-time communications – pushing data to one another as well as to individuals across the network – every machine identity must be continuously and effectively monitored and managed.

With the adoption of cloud computing, infrastructure-as-a-service (IaaS), and containerization, the days of manually managing machine identities are long gone because the number of certificates needed to secure machines has increased exponentially. And the manual issuance of certificates is a slow process. In contrast, code is used to quickly build and tear down machines. So, when application development teams are forced to manually request and configure SSL/TLS certificates, it can delay an otherwise fast application delivery. Automation is now critical in keeping machine identities secure and protected while maintaining delivery speed.

To meet this challenge, companies around the world are calling for greater adoption of automated Public Key Infrastructure (PKI) and digital certificate management to better align DevOps with security in these dynamic, highly scalable environments.
Building Trust with PKI

PKI is all about trust. How confident are you the data being accessed, the information being shared, and the content being downloaded is from a trustworthy source? Ensuring this layer of security is PKI – a broad array of policies, procedures, and tools that manage digital certificates and encryption.

The goal is to guarantee the secure transfer of electronic data – whether it’s transmitted via e-commerce, healthcare, banking and financial applications, or even internal applications. PKI is a commitment to delivering protection – helping to digitally sign documents, verify transactions, and create a framework of proof that sources and materials are trusted.

PKI is the mechanism by which verification takes place by assigning a pair of mathematical keys – one public and the other private. The public key is used by the client to encrypt, while the server leverages the private key to decrypt. This process of authentication keeps information safe and secure at all times.

The good news is this authentication process can be used across a broad range of scenarios – from email security and web communications to digitally signed software to file encryption/decryption. As long as the certificate authority (which issues digital certificates) and registration authority (which verifies user requests for digital certificates) are reliable, PKI security is almost always guaranteed.

This strong security and authentication can protect both people and machines. But to ensure PKI remains secure, keys and certificates must be properly protected and managed. While much attention has been paid to protecting usernames and passwords, far less has been dedicated to securing machine identities – a major target for cybercriminals. In fact, unsecured keys and certificates can be leveraged to steal confidential information, launch phishing attacks, and inject malware.

Machine identities can be especially challenging to manage given the continuous and rapid commissioning and decommissioning of keys and certificates that occurs in DevOps environments. Modern applications built using DevOps methodologies often rely on short-lived, ephemeral infrastructure that is torn down and rebuilt with every release. In these environments, machine identities are needed to harden the inside of the application – to encrypt container-to-container and service mesh communication. Without proper controls in place to secure all of these machine identities throughout every layer of the application, in every stage of production, bad actors can target the weakest link and pivot.

So how do you align DevOps with security, alleviating these challenges while supporting the processes of DevOps teams?
Without Standardized PKI Automation, DevOps Processes Suffer

Organizations must be able to identify, authenticate, and secure all machines – as well as their communications with other machines within and across hybrid cloud environments. To do this for modern applications built using DevOps workflows, automation is necessary and security should be treated as code. Any time spent by developers manually configuring or managing keys negatively impacts productivity and agility.

Unfortunately, instead of using automated security controls early in the development process, the solutions being put in place for machine identities in DevOps environments are often more like the “Wild West” than a structured protection system – with a range of disparate tools that differ by infrastructure type and environment. Why? Because DevOps teams often work in a silo and don’t want to risk being slowed down by security tasks. So instead, some rely on point products to generate self-signed digital certificates, while others tap into those offered by public cloud providers. Still others choose to keep everything in-house, creating complicated homegrown scripts or using insecure solutions built into existing DevOps platforms such as Kubernetes Secrets.

This stitch-it-together security approach creates a maintenance nightmare, is error prone, and enables the use of certificates that run counter to most corporate policies and security best practices (e.g., wildcard certificates, self-signed certificates). Developers end up spending far too much time on certificate issuance and installation, distracting them from their core competencies and delaying project timelines. Even worse, this approach just doesn’t work. Poor configurations increase the risk of breach and outages, while lack of oversight and governance means poor compliance with security and industry standards.

Put simply, there's got to be a better way for DevOps and the security world to work together.
The Way Forward: Secure PKI for DevOps, Without the Wait

Venafi and GlobalSign have collaborated to deliver a better approach. Partnering to seamlessly address the DevOps certificate challenge, the companies have built tight integrations across GlobalSign’s identity and security solutions and Venafi’s Machine Identity Protection offerings.

3 Pillars to Fast and Secure PKI for DevOps

*Venafi and GlobalSign make it easy to embed trusted machine identities into automated workflows.*

<table>
<thead>
<tr>
<th>Secure Provider</th>
<th>Policy Enforcement and Visibility</th>
<th>High-Speed Seamless Certificate Issuance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosted, trusted certificate authority</td>
<td>Service-oriented certificate delivery for seamless compliance</td>
<td>Native integrations with DevOps tools and supporting services</td>
</tr>
</tbody>
</table>

**Pillars for Secure PKI:** Venafi Cloud DevOpsACCELERATE and GlobalSign PKI for DevOps

Together, Venafi Cloud DevOpsACCELERATE and GlobalSign PKI for DevOps make it possible for developers to have quick, high-speed access to trusted machine identities for use across hybrid cloud infrastructure, containerized environments, and service meshes. DevOpsACCELERATE gives DevOps automated access to certificates within a set security policy, while GlobalSign’s cloud-based PKI services help developers, IT operations, and information security teams eliminate the need to build and manage CAs and supporting services.

Fueled by the power of DevOpsACCELERATE, DevOps teams now have out-of-the-box integrations – Terraform, HashiCorp Vault, SaltStack, Ansible, OpenStack, Kubernetes, Jetstack cert-manager, and more – to connect their toolchain to certificate issuance from trusted sources. Venafi additionally includes documented, standard interfaces for use across multiple client needs, including a REST API, open source VCert SDK, and ACME service.
A service that enables secure innovation across your organization.

One Integrated Service for Machine Identities: Venafi Cloud DevOpsACCELERATE and GlobalSign PKI for DevOps

The end result is one integrated service for machine identities, made accessible as a software-as-a-service solution. This common service makes it simple and fast for developers and IT operations to access the certificates they need, leaving the cryptographic details to the security and PKI experts. Security teams can set policy guardrails to scale certificate processes automatically, while maintaining certificate visibility for audits and compliance. The Venafi-GlobalSign integration makes it possible for modern applications to be built using DevOps methodologies while removing requirements for manual, time-consuming security processes. For enterprises of all sizes, the combined solution delivers:

- Support for DevOps workflows that require ultra-high-speed certificate issuance, with certificates issued in seconds.
- Certificate issuance integrated into the current developer toolset, including configuration management, container orchestration, release automation, and secrets management tools. Policy-enforced certificates are also embedded directly into CI/CD pipelines, aligning appropriate policies for each environment.
- Outage prevention through automated certificate lifecycle management, thus eradicating errors and enforcing security policies within DevOps workflows.
- Elimination of time-consuming, manual in-house PKI management or self-signed certificates.
- Ability to comply with standards such as the Payment Card Industry Data Security Standard (PCI DSS), National Institute of Standards and Technology (NIST), and the Health Insurance Portability and Accountability Act (HIPAA).
Venafi and GlobalSign make it possible to fully automate the procurement and installation of trusted digital certificates in the DevOps environment – driving the agility required for dynamic infrastructure, so developers can work faster, make smarter decisions, and be more productive.

Interested in learning more about putting the power of secure DevOps to work for your organization? Take a closer look at venafi.com/cloud.

About GMO GlobalSign

As one of the world’s most deeply-rooted certificate authorities, GlobalSign is the leading provider of trusted identity and security solutions enabling businesses, large enterprises, cloud-based service providers and IoT innovators worldwide to conduct secure online communications, manage millions of verified digital identities and automate authentication and encryption. Its high-scale PKI and identity solutions support the billions of services, devices, people and things comprising the IoT. A subsidiary of Japan-based GMO Cloud KK and GMO Internet Group, GMO GlobalSign has offices in the Americas, Europe and Asia. For more information, visit globalsign.com.

About Venafi

Venafi is the cybersecurity market leader in machine identity protection, securing the cryptographic keys and digital certificates on which every business and government depends to deliver safe machine-to-machine communication. Organizations use Venafi key and certificate security to protect communications, commerce, critical systems and data, and mobile and user access.

To learn more, visit venafi.com