Global Technology Provider Secures Code-signing Certificates to Safeguard Its Brand

Venafi Enables Secure and Consistent Code-Signing Certificate Control

Executive Summary
Industry | Computer Technology
IT Environment
Extensive use of security certificates for code signing as well as SSL, VPN and wireless access
Business Challenges
• Deploy consistent, automated IT security to maintain company brand
• Secure globally dispersed cryptographic keys and digital certificates
• Support production with centralized code-signing certificate security
• Protect against trust-based attacks
Solution Business Impact
• Safeguarded brand reputation using consistent security policies and practices
• Established a central, secure repository for code-signing certificates
• Automated security to support cloud deployments, time and resources, self-service, and consistent protection
• Conducted inter-department training for companywide code-signing, SSL, and other key and certificate security

Business Profile
As an early founder and international corporation, this organization delivers technologies for computers and communications. With a heritage of innovation, it continues to expand the reach and promise of computing while advancing the ways people work and live worldwide.

IT Environment
The company's IT environment supports over 100,000 employees and has billions of annual revenue. With employees in over 200 countries writing code, digital certificates for code signing have a significant impact on production, operations, and security. The organization also uses certificates for SSL, wireless, and VPN access.

Business Challenge
The company realized it needed consistent and automated key and certificate security to maintain the company brand. Many of the organization’s IT departments would benefit from this security, but the code-signing team took the lead. When the company’s code is signed using certificates, this is meant to confirm both the company as author and the integrity of the software. The company’s customers expect products signed with the company’s code-signing certificates to be secure—they must be able to rely on the brand to deliver safe products.
Attackers compromise code-signing certificates from legitimate organizations and use them to sign malicious code. Because the malicious code is signed with a stolen, legitimate certificate, it does not trigger any warnings, and unsuspecting users will trust that the application is safe to install and use. The company needed to protect its brand by implementing secure code-signing practices that prevent attackers from compromising its code-signing certificates.

With code being created by international development teams, keys and certificates for code signing were dispersed across the globe, often with one-off creation for particular projects. The code-signing team was faced with the challenge of securing all keys and certificates and ensuring consistent, secure processes moving forward. These challenges included ensuring attempts at automation did not copy the certificates inappropriately, managing certificate lifecycles, tracking certificate owners after people switch roles or companies, and providing a mechanism for provisioning new certificates. And after Heartbleed, the team realized it needed a solution that could quickly refresh and replace its key and certificate infrastructure if needed to remain secure.

“We have folks writing code in over 200 countries. This resulted in pockets of code-signing certificates all over the place and this was negatively impacting production,” said the solution architect. “The code-signing team needed a centralized system for key and certificate management and distribution.”

But more important than these operational challenges, the code-signing team had to ensure the security of certificates. “Malware uses a bunch of vectors to infiltrate systems,” said the solution architect. “We don’t want to be the owner of a certificate that was used to sign malware. We need to secure our business and brand as a trusted technology and security company—and securing the certificate-signing process needs to be part of that effort.”

Solution: Venafi

When the company decided that key and certificate security was critical to its code-signing project, the team reached out to their partners to ask what others were doing. Then at an RSA conference, the team went to learn more about their partners’ recommendations. Venafi was one of three recommended solutions that were pursued.

“One of the solutions we considered was a distant third. Another needed more work, which would have meant having to wait for additional development with APIs,” said the solution architect. “But with Venafi, the capabilities and agents we needed were already there. Out of the box we got what we needed instead of having to write our own interfaces. And it was only going to get better. ”

Solution Business Impact

Central, Secure Repository and Policy Enforcement

The primary business driver for acquiring the Venafi solution was the need to take the keys and certificates dispersed across the IT environment and put them into a central, secure repository protected by consistent policy enforcement. The code-signing team funded the Venafi solution, so the initial focus was to automate consistent key and certificate security for the code-signing managers.

At the company, the code-signing certificate mechanisms used in production are restricted for most use cases. Very few people at the company understand these restrictions and how to properly include code-signing certificates in the development process. To better manage this process, the code-signing team integrated Venafi with their Hardware Security Module (HSM). Using this integration, the company centralized their key and certificate repository, enabling central visibility and control, policy enforcement, and distribution for improved security.

“With Venafi, the code-signing managers can ensure that requests for code-signing certificates go through the sanctioned signing engine,” said the solution architect. “This gives us the control to do this the right way, the secure way.”
Comprehensive Visibility and Control
With Venafi, the company can establish a complete inventory of all keys and certificates. With this comprehensive visibility, the organization can ensure key and certificate security.

“Before Venafi, we were not doing a good job of remediating certificate expiration,” said the solution architect. “Certificates would expire and no one was managing it. Entire services would come down. With Venafi, we can see which certificates are about to expire and take a proactive approach.”

Workflows to Enforce Security
IT teams are also using workflows and approval processes to enforce policies, especially when individuals outside of the immediate managing group are part of the process. Before Venafi, the workflow practices were very basic. However, with Venafi, the teams can create more granular associations for ownership, actions, and approvals to ensure secure processes.

For example, application owners can be restricted to controlling the keys and certificates for their applications. And additional layers of restrictions can be established, such as limiting CAs, expiry dates, algorithm applied, and other criteria that impact secure key and certificate enrollment, provisioning and management. Also, the ability to associate a group instead of an individual to a particular certificate helps expedite a disaster recovery plan when needed.

“Venafi goes beyond enrollment to provisioning. The management team can configure the certificate options to ensure security and consistency, but then our internal customers can get their own certificates. This saves a lot of time—I don’t even have to touch it. When I heard that we could use Venafi for our SSL, code-signing, and my F5 load balancers, I said, ‘Sign me up!’”

Cross-team Training and Security
The code-signing team first engaged with the Venafi training team to view demos and confirm implementation for particular certificate security use cases. Now they are looking forward to getting more comprehensive training.

“During our upcoming training, we’ll be looking at detailed workflow capabilities and notifications. But we’ll also be looking forward to Venafi training that goes beyond the questions we can think to ask,” said the solution architect. “We want to really kick the tires and spark some ideas of other uses for our team.”

A broader view of the Venafi solution will also help to support internal sales pitches for funding—not only for staffing resources for Venafi implementation, but for the entire code-signing project.

The code-signing team wants to enable the Venafi benefits beyond their deployments. They struck a deal with other departments, agreeing to train a couple of people on their teams if they agree to implement and own the Venafi solution in their environments. The result—several other departments have expressed an interest in deploying the Venafi platform.

Network Team
Currently the network team is applying a patchwork of scanning and manual tools to manage their SSL environment and getting different results across these tools. Addressing these results requires iterations of scan, remediate, scan, remediate. The network team wants to use Venafi as a centralized key and certificate security tool that conducts holistic scans and provides near real-time information for their SSL environment.

Cloud Team
For the cloud team, they plan to leverage the automated processes in the Venafi solution. Currently key and certificate processes are conducted manually, which is slowing down their dynamic use of cloud computing. The cloud team wants to define policies in the Venafi solution, but then use the solution’s automated processes to securely provision and manage keys and certificates.

PKI Team
The PKI team is interested in developing a self-service portal that will enable others to provision their own certificates. With policies and workflows, the PKI team can implement consistent security and policy enforcement companywide, while freeing other teams to meet their own certificate needs.
**SAP Team**

As a team that hosts a large deployment of applications, the SAP team wants to streamline key and certificate provisioning and distribution. They deliver IT-as-a-service, which means they own the infrastructure piece, but they also need to help the owners of the applications with their key and certificate security.

The SAP team also supports applications with local and global load balancing, tying in the network team and requiring additional certificates across F5 LTMs. With application servers and load balancers, this team manages thousands of keys and certificates. They want the easy, automated, and secure certificate distribution and management processes delivered through Venafi.

**Automated Key and Certificate Security**

Across the various teams, automation is considered a critical feature of key and certificate security.

> We wish we’d had Venafi in place to remediate Heartbleed. At least now we know that we’re ready when a future vulnerability is discovered. Venafi lets us replace our infrastructure quickly if needed. Other departments outside of the code-signing team want to deploy Venafi to ensure they are also secure for the future,” said the solution architect.

Automation enables consistent deployment of secure processes and delivers time saving that can benefit all business groups. For the cloud services team, automation is essential to fully realize the dynamic benefits offered through a cloud environment. And other departments have a similar need for automated key and certificate security to support the capabilities of underlying technologies.

**Next Steps—SSL Certificate Portal**

For their next key and certificate security project, the company is looking to use Venafi for an enrollment and provisioning portal. Early on the team used a smart card provisioning tool, but it was limited to user certificates and did not help with pushing the certificates out to users. Next they created a homegrown portal with certificate options and approval workflows. But this portal was missing the distribution and control of certificates, and the company does not have enough resources to address this manually. The company will be replacing their current portal with Venafi.

“Currently we have a small team that manages all of the SSL certificate distribution. With the new Venafi portal, the team will maintain the automated structure, but the portal will provide self-service certificate provisioning,” said the solution architect. “Not only will the Venafi portal save time and resources, we’ll also have better security and control by restricting options in the portal. For example, if we need to get rid of a CA, we go into the tool and eliminate this CA as a choice. We can also see where this CA is already in use and take action.”

The Venafi portal will provide self-service SSL certificate enrollment, provisioning, and management while ensuring policy enforcement and security. As the company expands its use of Venafi beyond code-signing certificates, it further protects its brand reputation, securing the trust that keys and certificates establish as the foundation of safe business communications and authentication.

**TRUSTED BY THE TOP**

5 OF 5 Top U.S. Health Insurers  
5 OF 5 Top U.S. Airlines  
4 OF 5 Top U.S. Retailers  
4 OF 5 Top U.S. Banks  
4 OF 5 Top U.K. Banks  
4 OF 5 Top S. African Banks  
3 OF 5 Top AU Banks

**ABOUT VENAFI**

Venafi is the cybersecurity market leader in protecting cryptographic keys and digital certificates which every business and government depends on to deliver safe encryption, authentication and authorization. Organizations use Venafi key and certificate security to secure machine-to-machine connections and communications—protecting commerce, critical systems and data, and mobile and user access.

To learn more, visit [www.venafi.com](http://www.venafi.com)