digicert®

SECURING THE SOFTWARE SUPPLY CHAIN: SECURED CODE SIGNING AT SCALE

THE APACHE® SOFTWARE FOUNDATION apache.org

Organization

Site: www.apache.org
Industry: Technology
Headquarters: Dover, Delaware
Developers: 6,000

Key Challenges

The Apache Software Foundation needed to streamline code signing for 350 products and 6,000 developers on six continents, as well as manage SSL certificates for its servers.

Solution

- DigiCert® Software Trust Manager
- DigiCert CertCentral® Enterprise

Benefits

- Enhanced security for 6,000 developers on six continents with access to use but not download cloud-based signing keys
- Certificate-driven access avoids username/password management
- Minimized authentication risk with isolated and role-based access
- On-demand SSL certificates issued in minutes instead of days

The Apache Software Foundation develops and distributes 350 open-source software products critical to web services and support. When ASF needed better TLS/SSL certificate management and a simpler way to cryptographically secure, sign and validate authorship for these products, they turned to DigiCert for cloud-based code signing and SSL solutions. With DigiCert® Software Trust Manager and DigiCert CertCentral® Enterprise, Apache Software Foundation and their customers enjoy the trust of streamlined, secure code signing access for 6,000 developers on six continents, minimized risk, and on-demand SSL certificates issued in minutes instead of days.

A big impact

The Internet is changing the way we live and work, and the Apache Software Foundation is playing a major role in enabling that impact. ASF is a community of open-source developers formed in 1999, and its best-known product, the Apache Web server, is estimated to power more than 50 percent of all websites, including popular sites such as Apple, PayPal, Wikipedia and Alibaba.[1]

ASF develops and manages hundreds of other products, including Apache Hadoop for big data, the Apache Tomcat application server and Apache

[1] W3Techs, "Usage statistics and market share of Apache for websites," Retrieved April 2015

OpenOffice for productivity. "We're distributing this software for free, and people are building businesses either on it or with it," says David Nalley, Vice President, Infrastructure at The Apache Software Foundation. "When the Foundation was formed, open-source code was seen by many in the enterprise world with a little bit of mistrust. But now, 15 years down the road, more and more people are adopting it. OpenOffice has 100 million downloads."

How to stay open yet secure

A major challenge at ASF is maintaining the trust the organization has built. "Some people have abused our openness," Nalley says. "People have downloaded our code, such as OpenOffice, and bundled malware or adware along with it."

In an effort to validate authorship and guarantee there had been no tampering or alteration to the code, ASF employed a form of cryptographic signing for years. "The problem was that the way we were signing code was esoteric and required use of sophisticated PGP encryption tools for the user to verify the code was as intended," says Nalley. "Most users did not take advantage of this because they were not familiar with the cryptographic tools."

Nalley and team investigated options for improving the process, including building their own code signing software. "We also scoured the marketplace for solutions," says Nalley. "It took us a long time. Getting it right was important."

Cloud-based key protection

After considering a wide variety of solutions, ASF chose DigiCert Software Trust Manager. One reason was the degree of protection that Software Trust Manager offers for the digital keys used to sign code. If a key is ever lost or stolen, it can be used by cybercriminals to fraudulently sign code that includes malware.

> **"WE HAVE 6,000-PLUS DEVELOPERS ON SIX CONTINENTS. TRYING TO SECURE ALL THE KEYS THAT THEY NEED (FOR CODE SIGNING) WOULD BE A NIGHTMARE. WITH SOFTWARE TRUST MANAGER, THE KEYS REMAIN IN THE CLOUD, AND ACCESS IS PROVIDED TO SIGN WITH THEM, BUT NOT TO GET THE ACTUAL KEYS THEMSELVES. THAT IS A HUGE WIN FOR US."**
>
> David Nalley, Vice President, Infrastructure,
> The Apache Software Foundation

"One of the distinguishing features that we found with DigiCert Software Trust Manager is that people never get access to the keys themselves," Nalley says. "We have 6,000-plus committers—our term for developers authorized to write code—on six continents. Trying to secure all the keys that they need would be a nightmare. With DigiCert Software Trust Manager, the keys remain in the cloud, and access is provided to sign with them, but not to get the actual keys themselves. That is a huge win for us."

Critical control

ASF validates the identity of each developer authorized to sign code and enables them to acquire a user credential that gives them access to the keys that they need. "Thereafter, there is no user name or password involved," says Nalley. "We don't have to worry about lost, weak or forgotten passwords. Security is certificate-driven."

The solution provides role-based access to the keys that isolates them. "ASF administrators cannot sign any code," Nalley says. "And keys for one project cannot be used to sign another project. This protects against errors and misuse."

DigiCert Software Trust Manager provides a pool of rotating keys to each project at ASF, which minimizes business impact if a key is revoked. "We did need to revoke a key once, and because there are multiple rotating keys, it didn't affect the other releases signed by that project," says Nalley.

Visibility over compliance and spending

DigiCert Software Trust Manager also generates reports and audit logs that enable Nalley and other administrators to easily track and monitor activities. "The audit logs are incredibly helpful to us, and we go over them monthly," Nalley says. "We had a recent case where we saw someone signing strange files, and it ended up that the files simply weren't named in accordance with our best practices. We were able to investigate and find out that it wasn't a security issue."

The biggest win is for end users of ASF software. "Most platforms expect a user to have signed code, and there's an alarm if the user attempts to install unsigned code," Nalley says. "Now our users have a guarantee that the software actually came from ASF, and they have a better installation experience."

> **"WHEN WE WERE MANAGING SSL CERTIFICATES AD-HOC, WE HAD DELAYS AS LONG AS TWO WEEKS TO GET AN SSL CERTIFICATE. WITH DIGICERT CERTCENTRAL ENTERPRISE, WE GET THEM IN MINUTES NOW. IT'S A ONE-STOP SHOP FOR MANAGING, REQUESTING, RENEWING AND REVOKING CERTIFICATES ON DEMAND."**
>
> David Nalley Vice President, Infrastructure,
> The Apache Software Foundation

Authenticating servers in minutes instead of days

Just as software needs authentication from a trusted authority, so do servers. Secure Socket Layer (TLS/SSL) certificates perform this function. A Certificate Authority (CA) validates the owner of a domain and issues an SSL certificate for installation on a server.

ASF had been getting its SSL certificates from different Certificate Authorities on an ad-hoc basis. Each time, the certificate process required the CA to re-contact ASF and validate its identity before issuing or renewing the certificate in question. The process could take days, or longer.

And ASF had to monitor each renewal date and be sure that certificates didn't expire using a labor-intensive, manual process.

As the number of ASF websites increased, Nalley and team wanted to simplify SSL management. That's why they chose to deploy DigiCert CertCentral Enterprise, an enterprise-class, cloud-based certificate management console. With CertCentral Enterprise, an organization completes the authentication process just once by submitting organization details, domain name(s) and contact information, and answering a validation call. The validated data is then authenticated and stored, and from that point forward the designated customer contact can instantly issue DigiCert TLS/SSL certificates over the full life of the DigiCert authentication order.

"When we were managing SSL certificates in an ad-hoc fashion, we had delays as long as two weeks to get an SSL certificate," says Nalley. "With DigiCert CertCentral Enterprise, we get them in minutes now. It's a one-stop shop for managing, requesting, renewing and revoking certificates on demand." The biggest benefit from working with DigiCert is not just getting technical solutions, Nalley says. "Lots of people can solve a problem from a technical perspective," he notes. "It's that DigiCert also understands how to solve the process problem—how to be able to sign code or issue an SSL certificate within a large organization, empowering people to get things done while following guidelines. And that's delivering value to the organization as a whole."

About DigiCert

At DigiCert, finding a better way to secure the internet is a concept that goes all the way back to our roots. That's why our certificates are trusted everywhere, millions of times every day, by companies across the globe. It's why our customers consistently award us the most five-star service and support reviews in the industry. And it's why we'll continue to lead the industry toward a more innovative and secure future. In SSL, IoT, PKI, and beyond—DigiCert is the uncommon denominator.

2801 Thanksgiving Way, Suite 500 Lehi, Utah 84043. United States | www.digicert.com/software-trust-manager