CUSTOMER SUCCESS

The Apache Software Foundation

The Apache Software Foundation Simplifies Code-Signing for 4,000 Developers with Symantec Solution

The Apache Software Foundation develops and distributes 350 open-source software products that have proven critical to the web. It needed a simpler way to cryptographically sign them, validating authorship and security. It also needed to simplify SSL certificate management. It turned to Symantec for cloud-based code-signing and SSL certificate management solutions. Results included streamlined, secure code-signing access for 4,000 developers on six continents, minimized risk, and on-demand SSL certificates in minutes instead of days.

ORGANIZATION PROFILE

Site: www.apache.org

Industry: Technology

Headquarters: Dover, Delaware

Developers: 4,000

KEY CHALLENGES

The Apache Software Foundation needed to streamline code-signing for 350 products and 4,000 developers on six continents, as well as manage SSL certificates for its servers.

SOLUTION

The organization turned to Symantec™ Secure App Service, because it provides code-signing keys as a secure, cloud-based service, and Symantec™ Enterprise Managed PKI for SSL for cloud-based SSL certificate management.

BENEFITS

- 4,000 developers on six continents get cloud-based access to use, but not to download signing keys, enhancing security
- Certificate-driven access avoids username/password management
- Access is isolated and role-based to minimize risk
- 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 (ASF) 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]

The Internet's worldwide gross domestic product (GDP) has been projected to be US$8 trillion.[2] That means the Apache Web server helps to drive about US$4 trillion in value, an amount higher than the GDP of Germany or France.[3]

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

> "We have 4,000-plus developers on six continents. Trying to secure all the keys that they need (for code signing) would be a nightmare. With Symantec Secure App Service, 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

How to stay open yet secure

A major challenge at ASF is to maintain the trust that 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."

ASF has cryptographically signed its code for years to validate its authorship and guarantee that the code hasn't been altered or corrupted since it was signed. "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 how to improve the process, and evaluated 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

ASF chose Symantec™ Secure App Service. One reason was the degree of protection that Secure App Service offers for the digital keys that are 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.

"One of the distinguishing features that we found with Symantec Secure App Service is that people never get access to the keys themselves," Nalley says. "We have 4,000-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 Symantec Secure App Service, 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."

Symantec Secure App Service 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 on compliance and spending

Symantec Secure App Service 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 audit log also enables Nalley to see how often the solution is used. "Symantec Secure App Service has a policy of charging per signing event, meaning for everything that is signed at one time, as opposed to charging per piece of software signed," Nalley says. "We sometimes have many pieces of software in a release. The policy dramatically reduces the cost of providing the service."

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."

SOLUTIONS

- Symantec™ Secure App Service
- Symantec™ Managed PKI for SSL

Symantec

> "When we were managing SSL certificates ad-hoc, we had delays as long as two weeks to get an SSL certificate. With Symantec Managed PKI for SSL, 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 (SSL) certificates perform this function. A Certificate Authority (CA) validates the owner of a domain and issues an SSL digital certificate to be installed on a server. It generates the little green padlock that appears to the left of the domain name in the URL bar of the browser. The padlock indicates that a user has an encrypted connection, and that the domain name owner has been validated.

ASF had been getting its SSL certificates from different Certificate Authorities (CAs) 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 the ASF had to monitor each renewal date and be sure that certificates didn't expire.

As the number of ASF websites increased, Nalley and team wanted to simplify SSL management, and they chose to deploy Symantec™ Managed PKI for SSL. It's a cloud-based console for managing certificates across the enterprise. An organization can go through the authentication process just once, by submitting organization details, domain name(s) and contact information, and receiving a validation call. The validated data is then authenticated and stored, and from that point forward, the designated customer contact can instantly issue Symantec SSL certificates for the rest of the life of the Symantec 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 Symantec Managed PKI for SSL, 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 Symantec is not just getting technical solutions, Nalley says. "Lots of people can solve a problem from a technical perspective," he notes. "It's that Symantec 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."

For more information

Please contact your local Symantec Sales Representative or Business Partner, or visit:
go.symantec.com/secure-app-service or
symantec.com/ssl-certificates/managed-pki-ssl

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

[1] W3Techs, "Usage statistics and market share of Apache for websites", Retrieved April 2015
[2] Derek Thompson, "The $8 Trillion Internet: McKinsey's Bold Attempt to Measure the E-conomy", The Atlantic, November 2011.
[3] Wikipedia.com, "List of countries by GDP (nominal)", Retrieved April 2015

Symantec