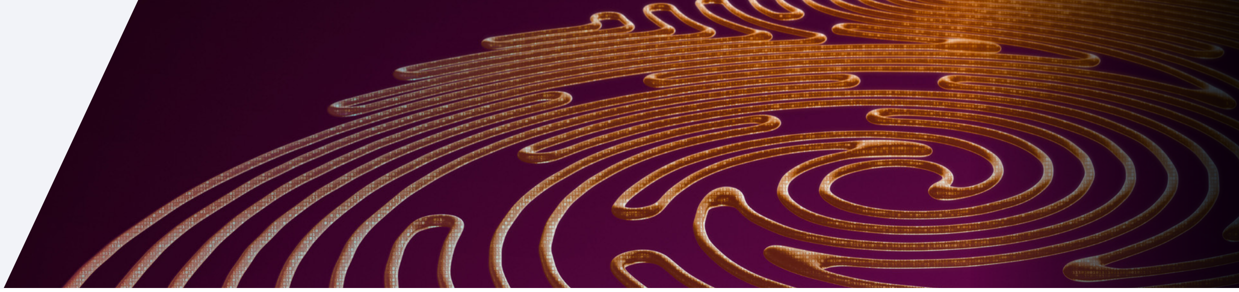

CASE STUDY

# Large bank uses Venafi to achieve crypto-agility; absorbs new acquisition without hiccups

## Challenge

A large national bank recently closed a deal to acquire a regional lender to broaden market share. The smaller bank had a strong reputation for customer service, and so the parent bank had no plans to consolidate brands. However, they did want to incorporate the regional lender's IT and cryptographic infrastructure into their own to enforce security policies and ensure compliance with federal and industry banking regulations.

The parent bank's InfoSec team quickly realized they had almost zero insight into the smaller bank's infrastructure. For one thing, they had no idea how many SSL/TLS certificates the smaller bank was using, let alone any insight into the locations, ownership or lifespans of these certificates. They already knew that the smaller bank used different primary certificate authorities (CAs) and that they would eventually need to migrate those certificates to the parent bank's approved internal and external CAs.

To complicate matters, the smaller bank's PKI lead admitted there was no automation in place to restrict which CAs could be used. "We had no way to ensure our app developers, for example, were using our authorized CA. I wouldn't have been surprised if they were using Let's Encrypt certificates for the sake of convenience," the PKI lead admitted.

Right before the purchase was finalized, the smaller bank experienced a certificate-related outage. Although the outage caused minimal damage, it underscored the urgency of gaining that necessary visibility.

## Solution: Venafi Platform

Fortunately, the parent bank had been a Venafi customer for several years and reached out to Venafi for help with the challenges they were facing. They were optimistic that the Venafi Platform, a CA-agnostic solution, could solve these challenges; however, they didn't know how long it would take.

Venafi studied the situation and drew up a success plan that would accomplish the combined bank's primary cryptographic goals:

- Get comprehensive visibility and actionable intelligence into the regional lender's TLS certificate inventory
- Incorporate the smaller bank's certificate lifecycle management into that of the larger bank
- Enforce security policies and business processes across the combined bank's infrastructure
- Achieve crypto-agility by migrating all remaining certificates to the parent bank's CA

Venafi told the customer that the first two goals could be accomplished within a month. The last goal probably wouldn't take more than a day—and that day could be selected at the customer's convenience—perhaps when the regional bank's contract with the other CA came up for renewal.

## Immediate visibility and intelligence into new population of TLS certificates

First, Venafi did a network discovery of all the regional bank's internal and external certificates. The total number of certificates Venafi discovered was almost double what the smaller bank's PKI lead had estimated. This discovery also gave the national bank actionable intelligence into all certificates at the regional bank, including location, ownership and expiration dates. The PKI lead's suspicion that app developers were using Let's Encrypt certificates in the CI/CD process ended up being correct.

The national bank also learned that the regional lender had been using wildcard certificates as machine identities for their F5 load balancers. The smaller bank had been using them because of the extremely time-consuming nature of replacing these certificates manually. However, this wouldn't fly in the parent bank's infrastructure because the latter's security policies did not allow for wildcard certificates.

After discovering and categorizing the regional bank's many certificates, Venafi helped the newly combined entity prioritize which certificates needed immediate attention.

## Automating certificate management fast

The top priority was to replace a wildcard certificate being used on several of the smaller bank's F5s because it was due to expire within the next two weeks. Using Venafi's automation capabilities and its native, out-of-the-box integrations with F5s, Venafi was able to replace every instance of this wildcard certificate with a single certificate for each individual load balancer from the parent bank's CA within a few days without interrupting service.

Then Venafi worked with the parent bank's InfoSec team and the acquired bank's PKI team to automate certificate management for all the smaller bank's current inventory of certificates. Whenever a certificate was due to expire, Venafi automated the certificate renewal process, replacing expiring certificates with new certificates from the parent bank's CA. The automated process ensured the new certificates were compliant with banking regulations and auditable. The Venafi Platform provided them with logs and other reporting capabilities that could prove their compliance to internal and external auditors.

Venafi also set up the same automated certificate lifecycle processes that the parent bank already used. This meant that the smaller bank's certificate owners had to follow the same protocols for procuring and consuming certificates and the same enforceable parameters—such as using only approved CAs and adhering to required configurations for certificates and private keys (including key lengths, algorithms and lifespans)—that the parent bank followed. If, say, an impatient developer tried to obtain a Let's Encrypt certificate, it would automatically be deleted.

However, there were no complaints from development teams. Venafi's many DevOps integrations and APIs made it easy for them to procure certificates through their preferred DevOps toolsets.

## Consolidating CAs using Venafi crypto-agility capabilities

Venafi was able to help the regional bank achieve their first two objectives with such speed and ease that they decided to accelerate their plans to migrate the remainder of the regional bank's TLS machine identities to the parent bank's CA. To minimize any possibility of downtime, the InfoSec team decided to make the switchover late on a Sunday night. The entire process took just a few hours. By the start of business Monday morning, the combined infrastructure of the two former banks shared the same external and internal CAs, the same machine identity management policies and processes and the same extensible solution set required to support planned digital transformation initiatives—all thanks to Venafi.

The InfoSec teams from both banks were amazed how quickly they were able to complete all the challenges they had identified using the Venafi platform. But they were even more impressed by the quality and quantity of help they received from the Venafi team. "They held our hands throughout every one of these initiatives and they went above and beyond the goals in our success plan. They also made sure that we would have the fastest, most efficient setup. You can't imagine how important that kind of support is when you're used to having your feet held to the fire," said the combined bank's director of InfoSec. "Venafi totally had our backs throughout the whole project. They were just as invested in its success as we were."