True Tales of 8 Certificate Outages

How to avoid disruption, distraction and downtime

VENAFI®

How bad can a certificate outage be?

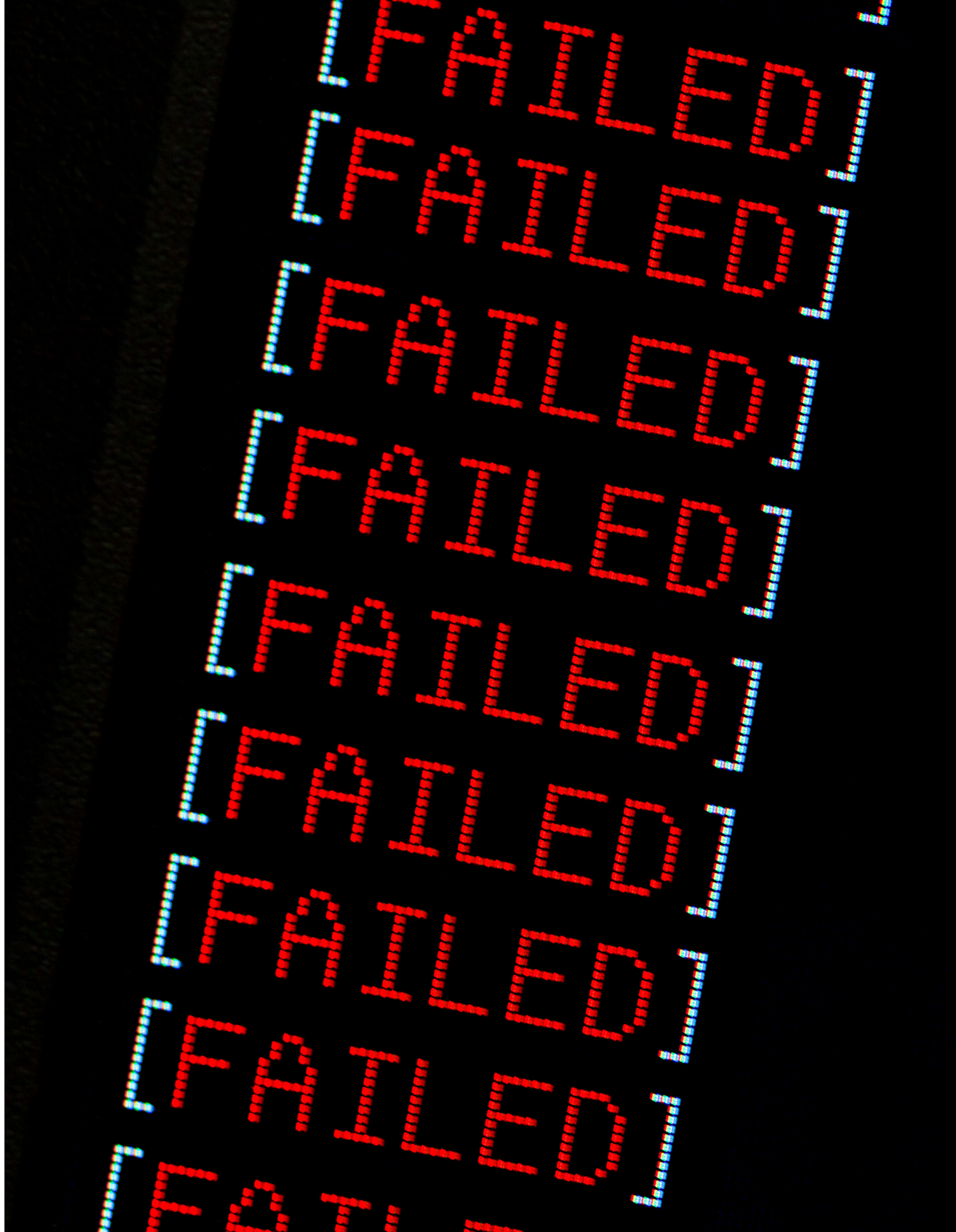
Certificate-related outages can easily become a disaster. The emergency-response clock starts ticking the minute an outage takes down servers or applications, delays revenue-generating opportunities and stalls productivity. But outages can even put people's lives at risk, such as when an expired certificate triggered an outage on the California Reportable Disease Information Exchange (CalREDIE) in 2020. That particular outage led to a massive undercount of COVID-19 cases reported in California, and prevented partners from uploading lab results to the CalREDIE system.

The impacts of outages can easily balloon as they become even more widespread. In 2017, Equifax was breached because of an expired certificate, compromising the personal financial data of almost 150 million Americans. Certificate outages at Microsoft brought down Microsoft Teams in early 2020 and Azure Active Directory in March 2021 which silenced Office 365, Dynamics 365, Xbox Live, Teams and other third-party apps. And these are just some of the high-profile outages that keep popping up.

Outages can be silent but deadly

For every newsworthy outage, there are thousands more that no one hears about. They wreak havoc across critical infrastructure in myriad ways—from toppling online storefronts to jeopardizing technological advances. And the panic and frustration of most, if not all, of these outages could have been prevented with a holistic, automated machine identity management solution.

Chances are you've picked up this eBook because your organization has weathered an outage or two, and you're looking to learn from the experience of others where to avoid outages. But more likely, you're seeking a way out of your ongoing problem with outages. We hope this eBook, which features eight outages suffered by organizations that later became Venafi customers, gives you confidence that this problem can be overcome.



Outage 1: Mobile banking app takes a social media hit

Lack of certificate visibility takes down a mobile banking app during a prime-time weekend

Over a holiday weekend, a bank's primary mobile app unexpectedly took a holiday of its own—right as bars and restaurants were filling up with people eager to celebrate. The bank's customers suddenly found themselves unable to pay for food and drinks, transfer money or even check their balance. Because the bank lacked visibility into their certificate inventory, they didn't find out about the problem until a dramatic uptick of scathing social media posts alerted them.

The root cause turned out to be an expired TLS certificate being used to authenticate a key microservice within the app. Because the certificate had been procured from an unapproved certificate authority (CA), the bank's homegrown certificate management tool had no information about it. After working around the clock over the weekend, a PKI admin finally located the certificate and resolved the problem—but not before the bank took a huge hit in direct revenues and brand damage from social media fallout.

TIP: Venafi helps you discover any rogue CAs being used in your network.

Outage 2: Interbank payment app's viability called into question

Multiple certificate-related outages threaten the future of an interbank payment solution

Originally developed as a peer-to-peer app, a FinTech firm's interbank payment solution had started to gain traction with institutional investors that needed a faster way to orchestrate payments to their customers. But as the app grew in popularity, it started to be plagued by certificate-related outages that restricted the number of transactions that could be processed.

At first these outages were sporadic and quickly remediated, but as the COVID-19 pandemic intensified, so did the frequency and severity of the outages. Their strategy for managing these machine identities—a hodgepodge of CA-based tools and manual processes—clearly wasn't working. Facing frustrated customers and angry banking partners, the FinTech firm knew they needed to overhaul the way they managed TLS certificate lifecycles, or risk losing customers, revenue and company viability.

TIP: Venafi helps you automatically renew and replace expiring certificates.

Outage 3: PKI administrator's dream vacation ruined

Expired wildcard certificate cuts short the holiday of a newly hired PKI leader

A manufacturing company's new head of PKI had a warning: The company's indiscriminate use of wildcard certificates would lead to outages. There simply was no way to know where all these wildcard instances were located without a comprehensive machine identity management solution in place. Upper management pooh-poohed her prophecy, having never experienced a serious outage themselves. After all, that was why they used wildcards—so they wouldn't constantly have to replace expiring certificates, which had always been a laborious process.

Eventually, she took a vacation that she had dreamed about doing for years. While relaxing by the resort pool, she received a frantic text. Believing something had happened to her boss, she returned the text—only to be told that a wildcard certificate managing multiple apps on one of the company's F5 systems had expired, grinding everything to a standstill. Being right was no compensation for having to cut her vacation short.

TIP: Venafi helps you discover which systems are using a given wildcard certificate.

Outage 4: Dozens of critical business systems forced offline

Major company allows a CA root certificate to expire before replacing intermediate certificates

A communications company relied on their approved CA to manage their certificates. When one of the CA's root certificates was due to expire in 60 days, the CA sent notifications to the company's staff. After all, when a root certificate expires, all the intermediate certificates issued under it expire as well. The company didn't replace the root certificate, so 30 days before its expiration date, the CA sent more notifications. The CA repeated the process at 15 days, seven days, three days, one day…

The root certificate expired, causing dozens of critical business systems to go down simultaneously. By the time the telecom discovered and remediated the source of the outage, they recognized how they had been warned over and over—and how the company lacked a strategy around escalation, causing the CA's warnings to come across as noise to ignore. But they couldn't ignore the consequences of their failure to respond. This massive outage led to unanticipated loss of revenues, including penalties for not meeting their licensing agreements.

TIP: Venafi helps you escalate notifications until they get the proper attention.

Outage 5: Brick-and-mortar retailer loses e-commerce sales

Expired certificate blocks customers from being able to pay for products

Several years ago, a national brick-and-mortar retailer experienced an outage on their new online storefront that rendered them unable to process payment card transactions. Customers either had to use PayPal or call the customer helpline to supply payment details over the phone. Rather than submit to such hassle, many customers abandoned their shopping carts in favor of the retailer's online-only rival.

The reason for the outage? An expired client certificate used to verify the retailer's software to the payment card provider service. Prior to the outage, the retailer had no idea that a certificate was involved in the payment card transaction process. When the application was originally installed and configured, the retailer may have been provided with detailed information about that certificate, but after several years, no remaining team members were aware that the ticking clock posed by that certificate's expiration date would one day result in the loss of millions of dollars in sales.

TIP: Venafi helps you locate unknown certificates across your organization.

Outage 6: An entire trading system goes down

A single certificate expiration causes the global outage of a trading system

One afternoon not very long ago, a leading financial services firm—the sort that manages institutional investments for other major financial institutions—was orchestrating their usual late-day heavy trading of stocks, bonds and assorted futures. As usual that day, many of their customers were making their trades near the close of business to hedge their bets.

Less than an hour before the markets closed, the firm's entire trading system went down. Customers could not even access the firm's system, let alone make their planned trades. The firm lost millions of dollars that day, as well as dozens of their customers in the days that followed. And the cause?
An expired TLS certificate.

TIP: Venafi helps you detect expiring certificates before they impact your business.

Outage 7: Priority for organ donation is taken offline

Certificate-related outage takes down the server hosting an organ donation list

A healthcare provider, whose primary-care hospitals performed organ transplants, maintained several organ-donor lists on their servers. But the organization was having multiple problems managing their TLS machine identities as more and more machines—everything from servers to implantable devices—were added to their network. Because they didn't have visibility into their certificate inventory, their systems were overrun with outages—more than 100 certificate-related outages in the previous year alone.

One of those 100 certificate-related outage turned into a life-or-death issue for the organization. When a certificate expired, the server housing the provider's organ donor priority list went down, delaying potential response. The provider had to reconstruct the list manually with the help of backup files, but someone in senior leadership admitted not being confident that everyone was accounted for. "People assume managing certificates is distinct from managing human identities. But as you can see, it really isn't," he said.

TIP: Venafi helps you prioritize where to focus certificate renewal efforts.

Outage 8: Certificate Expiration Notices Lost in Spam Folders

Expiring certificate notices were ignored or not received in the first place

Plagued by outages, a well-known specialty retailer set up their own certificate tracking system tied to Microsoft Active Directory. It incorporated some automation. Sixty days before a certificate was going to expire, they would send the owner of the certificate an email letting them know about the impending expiration. Typically, these emails either ended up in spam or were simply ignored.

Then, 30 days before a certificate's expiration date, they would open a ticket inside their ticketing system and assign a ticket to the certificate owner. For the most part, these tickets were ignored. At the 15-day mark, the InfoSec team would send an email to the manager of the certificate owner informing them that the owner hadn't responded to the ticket. Then they would spam the manager with emails until either someone took action or the certificate expired. Unfortunately, the latter was more common than the former—and the company realized their current machine identity management needed help—fast.

TIP: Learn more about the Venafi No Outages Guarantee on the next page.

Venafi Helps You Stop Outages in Their Tracks

Fortunately, the retailer from the previous example purchased the Venafi Platform as well as the VIA Venafi program to stop their outage problem permanently. VIA Venafi helped them to build an outage safety net to act as an early-warning system. In addition, Venafi helped them improve their notification processes by pinpointing the appropriate people to force immediate action before an outage can occur.

Moreover, Venafi turned certificate renewal from a series of cumbersome manual processes to a one-click process for the certificate owner. Venafi offers direct integrations with hundreds of systems, including F5 and other popular brands of load balancers, ticketing systems and commonly used DevOps tools. “Not having to worry about outages anymore has transformed the way we’re doing business,” said the company’s director of security.

Are you ready to eliminate outages forever—guaranteed?

You no longer have to weather the risks and indignities that certificate-related outages can pose to your business. Venafi can help. Contact us today to learn more about how we can help stop your certificate-related outages for good!

Get a free technical consultation or visit **venafi.com/outages** to learn more.

VENAFI®

About Venafi

Venafi is the cybersecurity market leader in machine identity management, 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