
#PKIPROBLEMS
7 reasons why teams fail at PKI and certificate management
(and what they can learn from Reddit)
PKI ADMIN
KEYFACTOR

A DAY IN THE LIFE

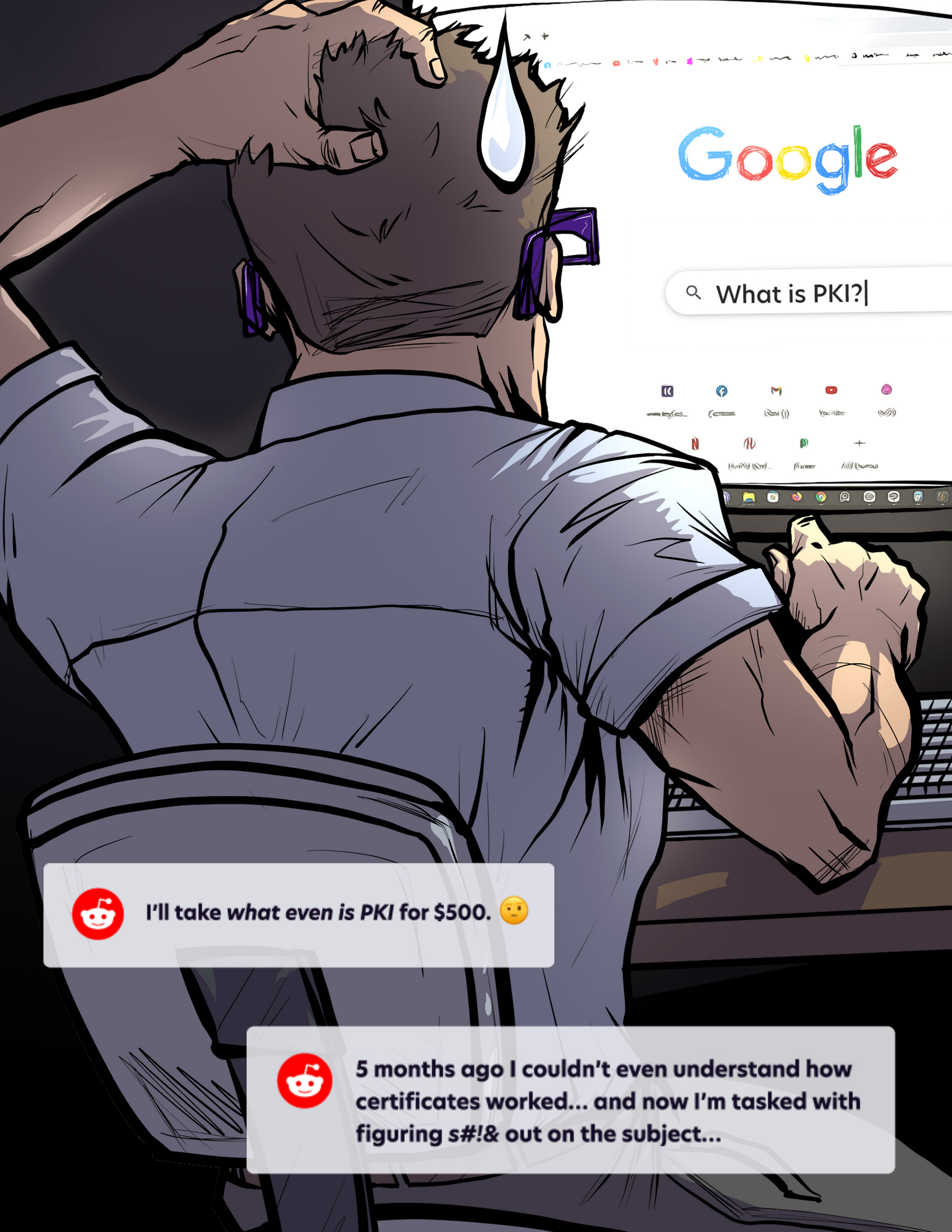
Whether public key infrastructure (PKI) is your passion or it's something you wouldn't touch with a 39-and-a-half-foot pole, it's without a doubt become critical to the security of your organization. A rare few companies have an in-house expert or even an entire team dedicated to PKI, but for most, it's more of a "hot potato" that gets passed to anyone brave enough to take it on.

At Keyfactor, we interact with these brave souls every day. We hear their frustrations, we feel their pains, and we've made it our sole purpose to help them overcome even the biggest PKI challenges. That's why we compiled this eBook. Inside these few pages, we've identified the 7 most common reasons why teams fail at PKI and certificate management. Our goal is to shed light (and a bit of humor) on the ups and downs of a day in the life of a "PKI admin", and to share lessons learned from those that have taken to Reddit to vent about all their PKI frustrations.

That's right. We took a deep dive into the endless universe of subreddits to find only the best, the bitterest, and yes, even the baddest posts from PKI admins on Reddit. We hope you'll draw as much enjoyment as you do insight from their words.

Warning

Some Reddit posts included in this eBook use strongly worded language. To keep our legal team sane and avoid making this eBook a Quentin Tarantino-style monologue, we've kindly redacted any coarse language for you. We'll leave it up to you to put two and two together.


Google
What is PKI?
I'll take *what even is PKI* for $500.
5 months ago I couldn't even understand how certificates worked... and now I'm tasked with figuring s#!& out on the subject...

01 LACK OF EXPERTISE

PKI heroes aren't born, they're made. It's a path less travelled for most, but for the few that dare to take it on, it's rarely by choice. PKI is one of those things that often gets relegated to any IT admin willing (or not) to do it. To add insult to injury, the tools organizations use to implement PKI usually require in-depth knowledge and provide minimal documentation. And since there's no "hitchhikers guide to PKI," the next best thing is to turn to Google to figure it out. Even if you are a PKI master, your certificate users aren't. They make mistakes and ignore policies. As much as you try to stay ahead, it's just not possible for a small team (often a lonely team of one) to help with every certificate-related task, not to mention all the other plates you're spinning.

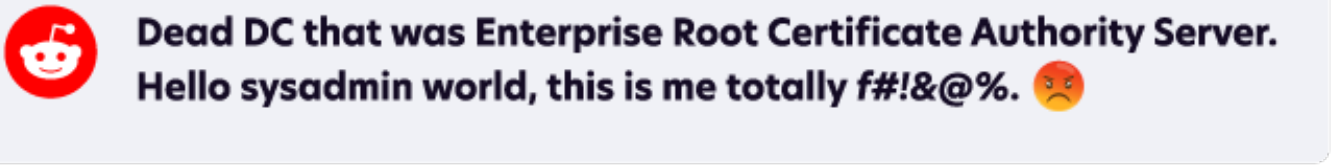
LESSONS LEARNED

If you want to know the average weight of an Elephant, Google away. If you want to find sound advice for setting up a proper PKI, then Google may not be your best bet. In fact, it can quickly lead you down a rabbit hole of misinformation. So, before you go down that road, take a hard look at the scope of your PKI deployment and consider if you've got the expertise, time, and the patience (oh, so much patience) to take it on. If the answer is no, it may be time to bring in re-enforcements or make the case for PKI as a Service.

02 PKI MISCONFIGURATION

Getting an internal PKI up and running isn't as straightforward as it looks. It's just too easy to hit that "next" button and skip by default configurations without considering what it means for your organization. If you've ever underestimated the weight of these configuration decisions made early on, you've learned this the hard way.

PKI is just one of those things where you have exactly one chance to get it right – at installation. Once you've issued your first certificate, there's no easy way to reverse course without a complete rebuild. PKI isn't exactly "set and forget" either, it needs regular care and feeding to keep it healthy, operational, and secure.



LESSONS LEARNED

Okay, so your PKI isn't going to explode. Point is, setting up your PKI is a marathon, not a sprint. It's also more than just CAs and certificates. When teams rush deployment, they often make one of two mistakes (or both). They focus too much on CA hierarchy, resulting in overly complicated PKI designs that involve more CAs than necessary. Or they under-architect everything else — things like CRL distribution points, backup and disaster recovery, security of the offline root, certificate policies, validity, key sizes, and signing algorithms – all the critical components that go into a well-architected PKI.


AD CS Configuration
DESTINATION SERVER
AD.SC.LAB
Setup Type
Specify the setup type of the CA
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.
Enterprise CA
Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.
Standalone CA
Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).
Previous
NEXT
PKI ADMIN
PKI is one of those things that is easy to do, but just as easy to do wrong. And if you don't figure out it's wrong early, it's a real pain in the a%$ to fix.
Yup, our CA got nuked a few weeks ago and are in the process of repairing it. Fun times.


EXPIRED
CERT!

03 LIMITED VISIBILITY

Monday morning rolls in, you grab a coffee to start the day. Let's face it, you'll need it. If you're responsible for tracking certificates, putting out fires is just another day on the job. Spreadsheets are one way to do it, but there's always that one certificate that gets away from you. Where is it installed? Who owns it? What if they've left the company?

It's like a never-ending game of "whack a mole." No matter how many monitoring tools or rows and columns you drum up, expired certificates unexpectedly pop out of the woodwork. Just when you think you have things under control, it happens again. Another untracked certificate expired and it's your job to chase it down and fix it.

G@&%$!# CERTIFICATES EXPIRING 😡 AAAAAAAARRRRGGGHHH
Seriously, why can't they just never expire. Every g%#$@#! thing seems to need a thousand of them and they always expire before you can catch them.
Got monitoring? *BOOM* there's one you didn't monitor. 😒

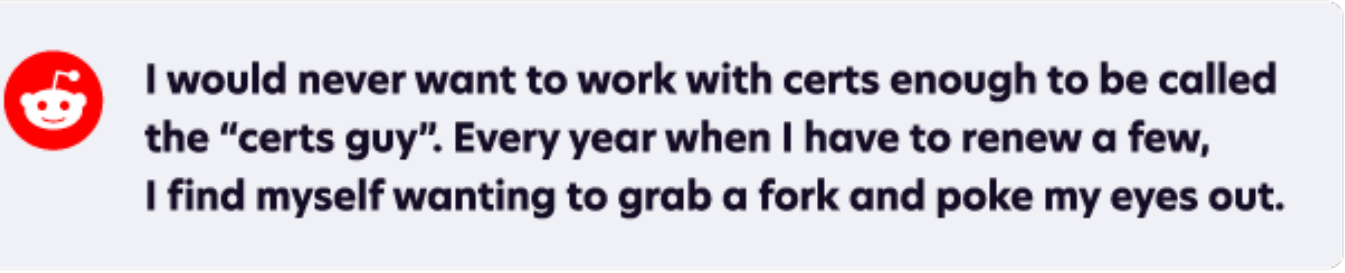
LESSONS LEARNED

It's not the certificates you know about that cause the biggest headaches, it's that one certificate you didn't see. You know...that one certificate that one admin installed on that one load balancer last year. You know where it is, right? If you're still using spreadsheets, probably not. To get a full and accurate inventory, you need visibility into (1) CA databases, (2) SSL/TLS endpoints on the network, and (3) key and certificate stores. If you don't have visibility from the CA down to the cert store, it's difficult to detect any unexpected changes.

04 MANUAL PROCESSES

Engineers and developers are busy too, but their focus is on delivering new features and keeping things running, not certificates. The problem is that people are, for the most part, not good at anything they only have to do once in a blue moon, and installing certificates just isn't something they do often.

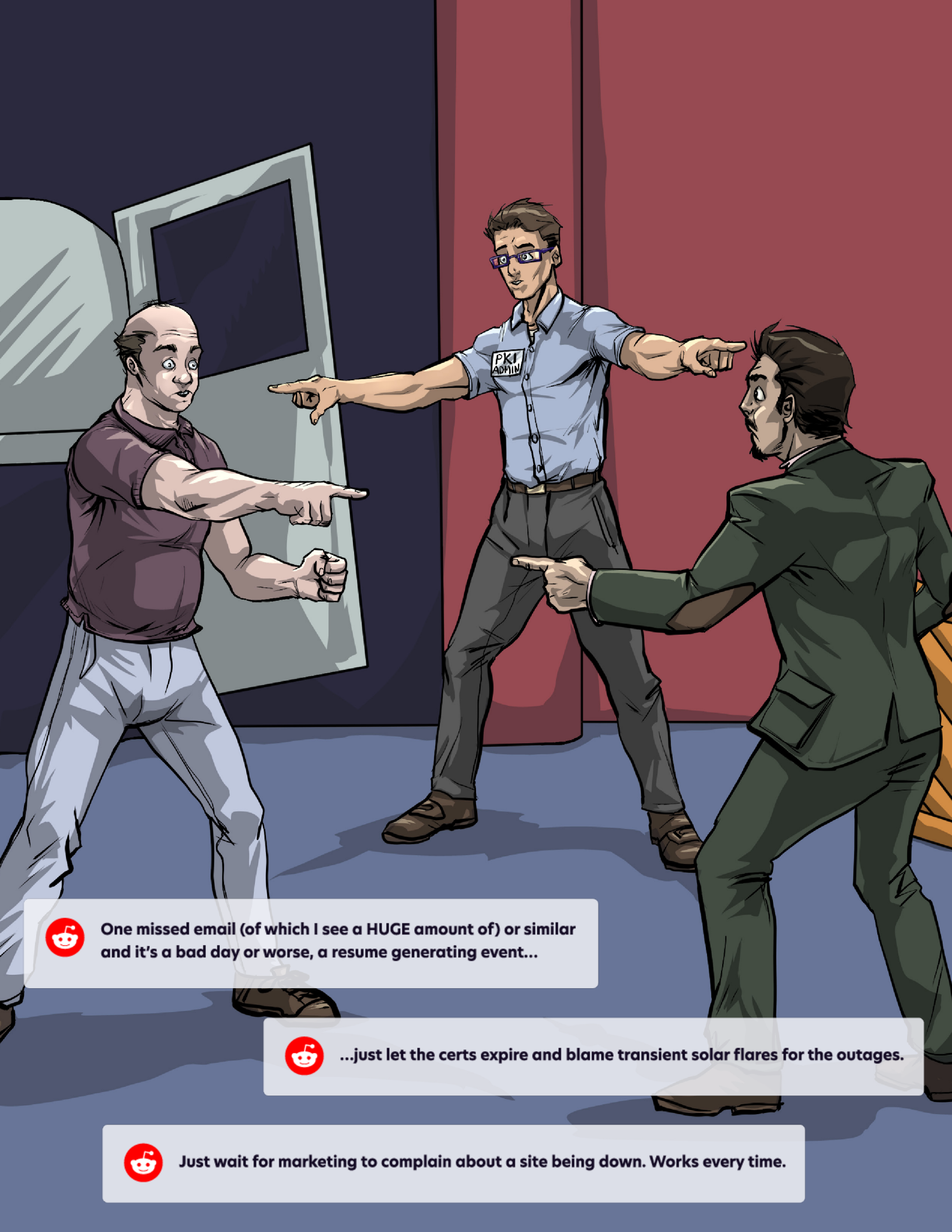
They might install a certificate once, swear they have it figured out, maybe even document it, then move on. A year goes by and suddenly they forget how they did it. So, when they get notified about a soon-to-expire certificate, they renew it and install it onto a server. Done, right? A few days later, there's a SEV1 outage. Turns out they forgot to bind it to the website.



LESSONS LEARNED

Certificates are a source of frustration for many. If you're the sole person responsible for issuing and approving certificates, keeping up with requests can feel impossible. For end-users, manually renewing and installing certificates is just as painful. It's a mind-numbing process of trial and error, but there's no need to resort to self-injury (seriously, put the fork down). Using automation tools, including standard protocols (e.g., ACME) and certificate lifecycle management solutions, can reduce errors and hours of repetitive tasks.


CERTIFICATE HELPDESK
PKI ADMIN
TAKE A NUMBER
STILL haven't figured out the process to get certificates installed without putting my hand in a blender.
I LOVE renewing certificates! Said no one ever...
F#!%. Certificate. Renewals. That is all. Horrible part of my job, times 200 plus.



One missed email (of which I see a HUGE amount of) or similar and it's a bad day or worse, a resume generating event...

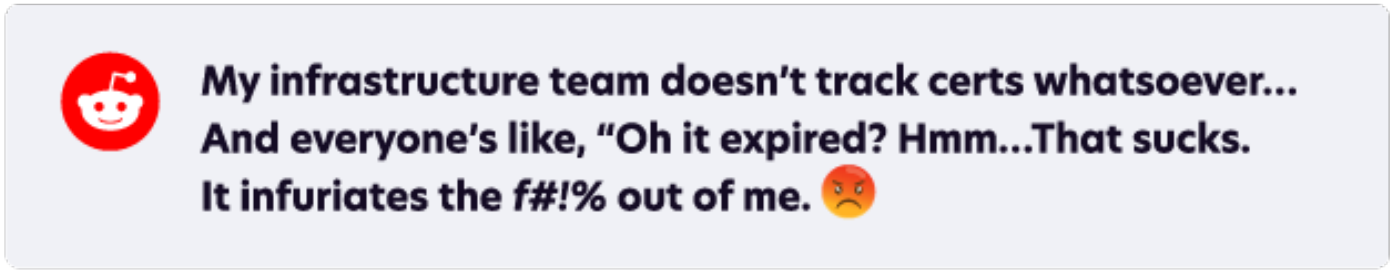
...just let the certs expire and blame transient solar flares for the outages.

Just wait for marketing to complain about a site being down. Works every time.

05 NO CLEAR ACCOUNTABILITY

If a certificate expires, and it don't look good, who you gonna call? No, it's not the Ghostbusters. If only the answer was that simple. The reality is that certificate-related outages often trigger a frenzy where teams scramble to find the expired certificate and renew and replace it on who knows what server or how many (wildcard, anyone?).

So, who or what do you blame? When it's all said and done, the hammer unfortunately often drops on the PKI owner, despite the barrage of emails and IMs they sent to the certificate user to renew their certificate. Once the outage is fixed, everyone moves on without so much as an "oops, sorry." It's no wonder no one wants to be "certs guy."

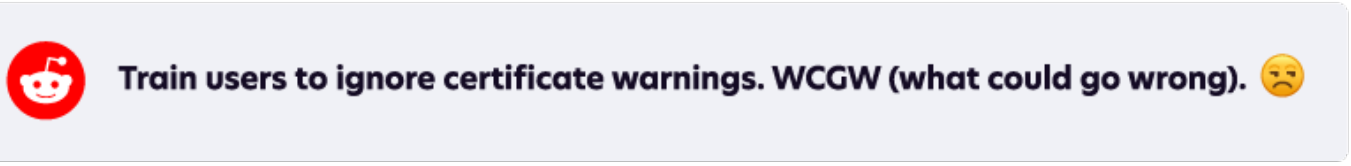


LESSONS LEARNED

If you want to avoid the blame game, it's important to define clear ownership between PKI operators and certificate managers, approvers, and users. It's equally important to monitor for expiration and alert users (and sometimes, their manager) well in advance. Automating expiration alerts, and the renewal/provisioning process altogether, can prevent these situations and ensure that there are clear lines of accountability without chasing down certificate owners. No more email blasting, no more calendar reminders.

06 UNRESTRICTED ISSUANCE

Certificates aren't just commodities, they're critical security infrastructure. The problem is that there's no one way to get a certificate. In fact, there are many... too many. And just like water, users will often find the path of least resistance to get the job done, which usually means getting their hands on a certificate without documenting it, or worse, issuing self-signed certificates in production. They may even stand up their own CAs and start spitting out certificates with no way to ensure that they're trusted or compliant. It's not unlike the wild west, where "outlaw" admins do their own thing without any oversight, and it becomes a nightmare to keep things under control.



THE THING ABOUT BUILT-IN CAS

Certificate issuance capabilities built into tools like Kubernetes, HashiCorp Vault, or VMware vCenter are easy to set up, but you need to consider where those certificates are used and what level of assurance they require. At minimum, you'll need to monitor issuance and expiration. More importantly, if certificates are used in production environments, it's better to integrate these tools with a trusted enterprise-run PKI for certificate issuance.

LESSONS LEARNED

The harder it is for application owners to request and issue certificates, the more likely they are to seek out alternative, non-compliant ways to obtain them. Consult with your application and operations teams to understand how they're leveraging certificates and how best to support them. Ideally, leverage a certificate management solution that provides self-service UI, APIs and plugins to their native tools and workflows.


PKI ADMIN
OpenSSL
Cryptography and SSL/TLS Too
ANSIBLE
Last job I had was a nightmare of expiring certs.
We had 5 registrars, and over 3000 domains.
The policy was “if you need a cert, just buy one”...


Especially f#!% lazy sysadmins that scatter wildcard certificates literally everywhere and not document where, so when that bad boy's ready for expiring, the whole ordeal becomes an imperial clusterf@&! of epic proportions. 😑

07 WILDCARD CERTIFICATES

Wildcard certificates are meant to save time and money, but when admins don't keep track of them, that's where things go wrong. If just one server hosting a wildcard certificate is compromised, all other servers are put at risk. Worse yet, if that one certificate expires, it's game over for uptime.

Take a lesson from the Empire. All it took was one blast from Luke Skywalker to bring the entire Death Star crashing down. Just like that exposed thermal exhaust port, if a wildcard certificate is left unprotected and unmanaged, it creates a single point of failure that could bring down the network.

NOT A STAR WARS FAN?

Let's look at a real-world example. On April 6, 2021, Epic Games experienced a global service outage that impacted everything from popular games to their online store. Logins failed, players were disconnected, store purchases halted, and gamers took to Twitter to vent about it. It took more than 25 people, 5.5 hours, and countless Zoom calls before systems were fully restored. What triggered the outage? A service-to-service wildcard certificate unexpectedly expired; that one certificate was installed across hundreds of different production services. Thankfully, Epic Games shared their story publicly to help others avoid the same fate.

LESSONS LEARNED

Avoid wildcard certificates, and never use them on production systems. It may seem cheap and convenient to fire one off to multiple servers at once, but when it comes time for renewal, getting every server updated at the same time while avoiding high traffic service windows can be extremely difficult to co-ordinate. Not to mention the security risks, such as the ALPACA technique recently highlighted by the NSA. If you're on the PKI or security team, getting an understanding of the scope of each wildcard certificate and how you can start to replace them over time is critically important.

SO, WHAT NOW?

It should come as no surprise that more than half of companies (55%) say they don't have enough staff dedicated to their PKI and another 88% continue to experience disruptive outages caused by expired certificates. Just thinking about these PKI problems is enough to give you a headache.

The good news is that the technology behind PKI and certificate management has advanced dramatically in the past few years, and many companies have now shifted to a cloud-first approach.

At Keyfactor, we've developed an end-to-end platform to simplify PKI just the way you need it, whether it's on-premises, in your cloud, as turnkey SaaS, or even fully managed PKI. Even better, we combine our PKI solutions with end-to-end certificate lifecycle automation, so you can discover and manage every certificate issued from any CA, any cloud, anywhere.

Like fast-acting Advil to that pounding headache, we work with customers big and small to solve even the most complex PKI problems. Whether it's migrating companies from their legacy Microsoft ADCS to a highly scalable SaaS PKI, integrating DevOps tools with certificate automation, or just getting an accurate inventory of certificates to stay ahead of outages. There's no PKI problem too complex for us to solve.

So, if you're ready to leave your PKI problems behind, it's time to take the next step. You can check out a product demo (no forms, no fuss), learn more about our solutions, or talk to one of our experts today. The next step is yours to take!

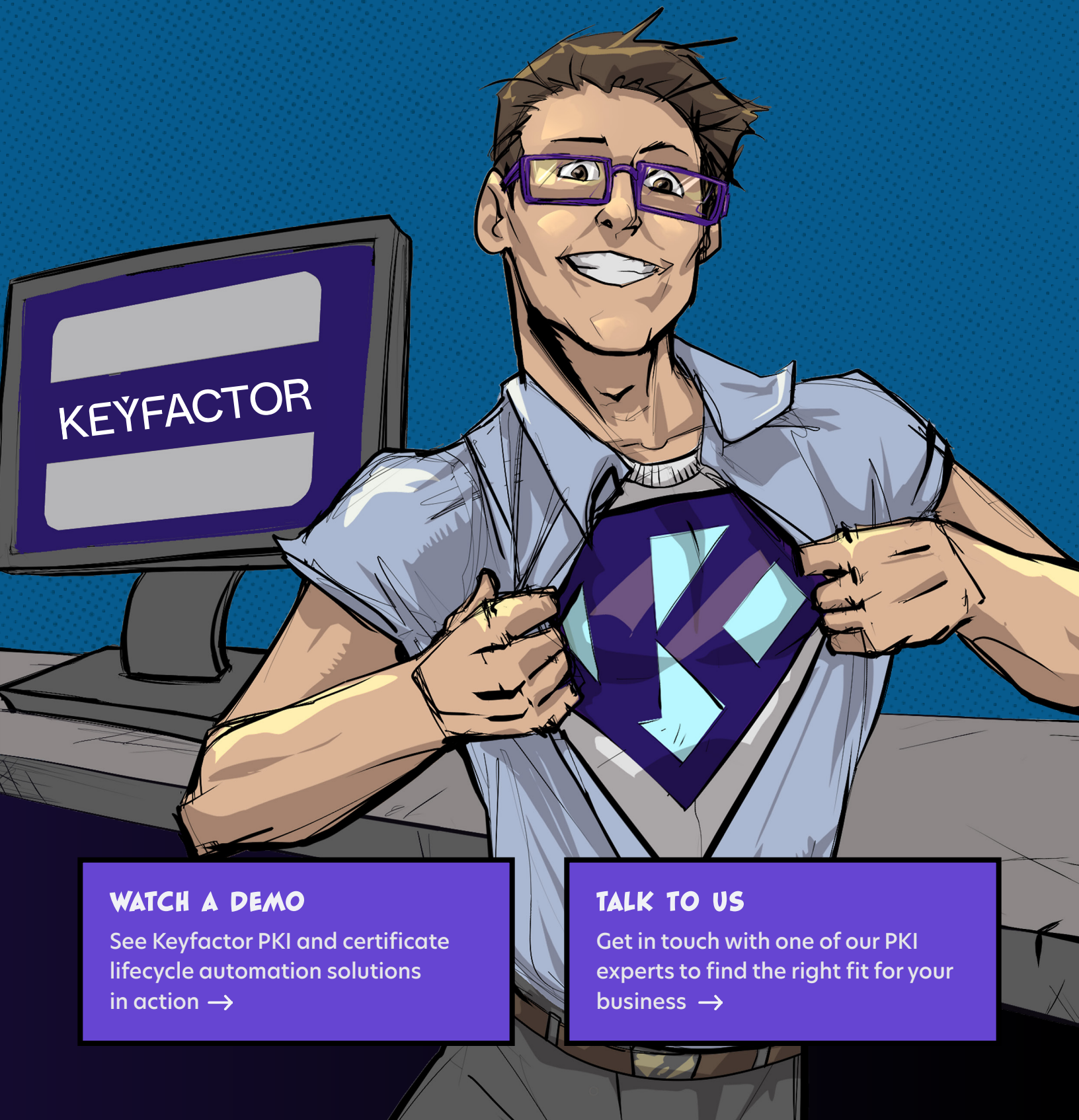
DISCOVER PKI SOLUTIONS

Learn about Keyfactor PKI solutions in the cloud, as a service, or on-premises →

DISCOVER CLA SOLUTIONS

Learn about Keyfactor Command for CA-agnostic certificate lifecycle automation →

LEAVE YOUR #PKIPROBLEMS BEHIND



WATCH A DEMO

See Keyfactor PKI and certificate lifecycle automation solutions in action →

TALK TO US

Get in touch with one of our PKI experts to find the right fit for your business →

KEYFACTOR

Keyfactor brings digital trust to the hyper-connected world with identity-first security for every machine and human. By simplifying PKI, automating certificate lifecycle management, and securing every device, workload, and thing, Keyfactor helps organizations move fast to establish digital trust at scale — and then maintain it. In a zero-trust world, every machine needs an identity and every identity must be managed.

For more, visit keyfactor.com or follow @keyfactor.

CONTACT US

- www.keyfactor.com
- +1.216.785.2946

ILLUSTRATOR

Matt Erkhart: erkhart.com