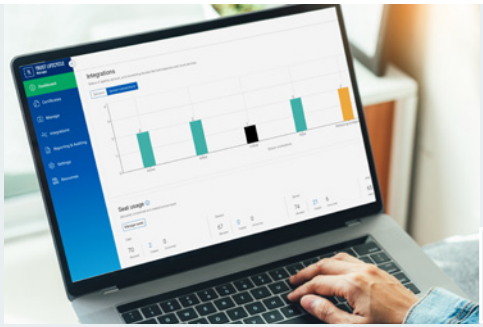


EBOOK

CAN YOUR CURRENT CLM TOOL HANDLE ALL YOUR PKI CHALLENGES?

Maybe it’s time to replace it with a comprehensive PKI management platform.

digicert®

TABLE OF CONTENTS

INTRODUCTION:

THE LIMITATIONS OF LEGACY CLM TOOLS

Many organizations, particularly larger companies in the Global 2000, have more than a passing acquaintance with certificate lifecycle management (CLM) tools. And most of them, particularly those in highly regulated industries like financial services, healthcare, and the public sector have been using dedicated CLM tools for years to manage their burgeoning population of digital certificates. They understand the value of leveraging the security potential of PKI to protect their corporate resources.

Increasingly, however, these organizations are discovering that their legacy CLM tools aren't up to the task of tackling the myriad challenges posed by their complex IT environments. For example, legacy CLM tools claim to have integrations with third-party devices and tools—but most of those integrations work only as isolated systems with the CLM tool itself. Because the integrations don't allow for linking with other third-party machines, they can stymie the ability to create complex workflows of which they should be a part.

In order to obtain even a semblance of cross-compatibility, organizations typically require the help of a CLM vendor's professional services team to make them work. Hiring this help is not only expensive, but it also doesn't guarantee that these workarounds will perform the same way in similar scenarios—particularly those in other IT silos that lack the PKI expertise to see that their problems all stem from the same root cause.

This eBook shows how six seemingly unrelated challenges revolve around this one issue and why your organization needs a full-stack, end-to-end solution that not only manages all your digital certificates but also the PKI infrastructure that enables their use. We're using a leading North American bank to better illustrate this state of affairs—but the challenges described in the following pages are ones that security-conscious companies in all industries can appreciate.

CHALLENGE 1:

WE CAN'T FIND ALL OUR DIGITAL CERTIFICATES

The outage happened early on the last day of the month, right when the bank's commercial customers most needed access to their accounts. Several businesses couldn't make payroll. Others couldn't pay their creditors. And some companies, whose fiscal year ended on that day, couldn't access the statements and reports they needed to pass their financial audits.

It took almost 24 hours for the network administrator to find and report the root cause: an expired TLS certificate used by an API gateway to secure and encrypt communications between the bank's internal services and their client applications. The outage ended up costing the bank several million dollars due to cash flow disruptions and operational delays.

Feeling blindsided, the director of IT contacted the bank's CLM vendor. The vendor apologized for the lapse, although they noted that discovery of most internally issued certificates required a managed PKI tool that would cost extra and require the vendor's professional services team to deploy. But it wasn't clear how this tool would help her team achieve complete visibility of the bank's entire population of public and private TLS certificates.

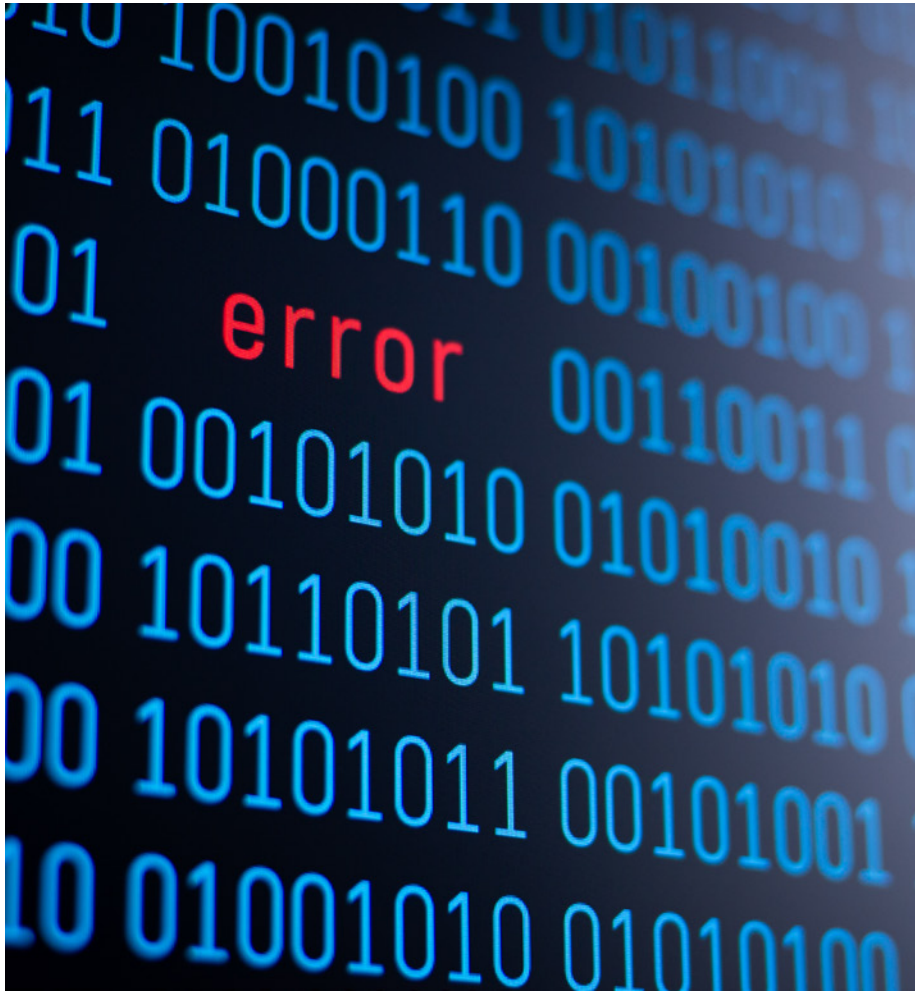
"Is this something we get to look forward to every time our infrastructure evolves?" the director wondered. "The whole point of having a CLM solution is so we don't have to deal with situations like this!"

Tools needed: Turnkey digital certificate discovery and provisioning across the bank's entire IT infrastructure even as it grows and modernizes; a centralized, continuously updated inventory of the bank's complete digital certificate population.

"The whole point of having a CLM solution is so we don't have to deal with situations like this!"
– Director of IT

CHALLENGE 2:

DON'T MAKE US CHOOSE BETWEEN SPEED AND SECURITY



The bank's application developers were getting frustrated. Already under so much pressure to roll out new updates and features, they struggled—and often failed—to uphold corporate security policy.

The lead DevOps architect couldn't fault the development teams. After all, every app the bank rolled out was constructed from hundreds of microservices built by multiple teams using disparate programming languages—and every single one of these microservices needed a machine identity to authenticate and communicate with one another. These digital certificates had to work across multiple containers to enable cloud-based workloads, and they often were ephemeral, living just long enough to make the necessary connections.

"No sane developer wants to put out insecure code," said the architect. "But we're not being paid to be security experts. They're paying us to push out new apps and features as fast as possible. I get that InfoSec doesn't know our workloads and development environments, but they need to start working with us instead of against us."

The bank's current CLM vendor did have a new tool that addressed managing machine identities in cloud environments; however, the tool didn't offer the ability to dynamically spin up ICAs (Intermediate Certificate Authorities) that would facilitate security across multiple workloads without having to rely on certificates issued by external CAs like Let's Encrypt.

Tools needed: Automate provisioning of machine identities in cloud native environments; dynamically spin up ICAs that can securely issue ephemeral certificates; remove the burden of security so developers can focus on core development responsibilities.

CHALLENGE 3:

ACCESS TO OUR DATA IS NEITHER SEAMLESS NOR SECURE

"We reached out to our CLM vendor to discuss the problem, but they told us they don't handle client certificates. Where does that leave us?"
– Senior IAM Admin

The senior IAM (identity and access management) administrator was dejected. Each day seemed to start with at least a few panicked employees who couldn't log into their corporate email account on their new iPhone or couldn't access data they had only recently been given access to. Reprovisioning their account to reflect that privilege took time—time often spent helping the others on help desk calls. Sadly, he was used to that. What sent him down a funnel of futility was the phone call from his buddy, a former colleague who now worked for a competitor. "He said, 'Hate to tell you this, dude, but I can still access the network. Just giving you a heads up because if you haven't revoked my privileges, there's a good chance you have other people who can, too,'" the administrator recounted.

The truth only confirmed his suspicions. If they couldn't assure continuous access for current employees, it would follow that they couldn't reliably revoke it for terminated ones. His team had no visibility into the client certificates used to authenticate users, which meant they often first learned of an expired client certificate when an employee called the help desk. The tools and scripts his team were using didn't integrate well with the bank's mobile device management (MDM) solutions, so that every time the latter had an update, they had to work overtime to preserve the connection. As a result, they risked failing to properly enforce corporate security policies on users' mobile devices.

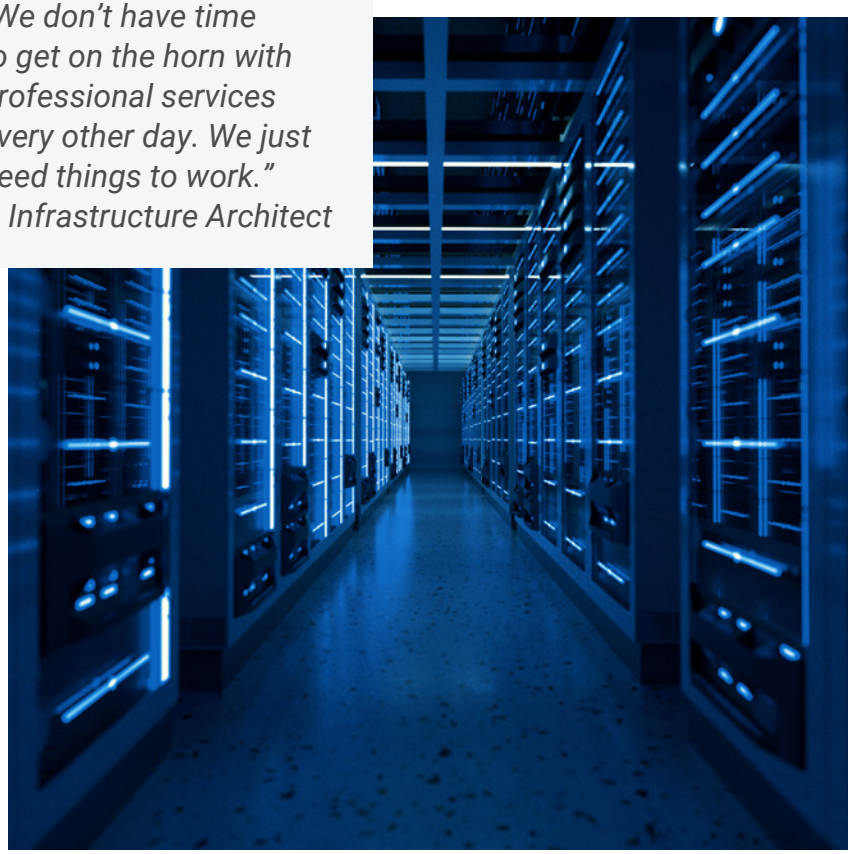
"We reached out to our CLM vendor to discuss the problem, but they told us they don't handle client certificates," said the administrator. "Where does that leave us?"

Tools needed: Enable current employees to seamlessly access corporate apps and data, based on role; Automate access throughout the employee lifecycle, from onboarding to termination; provide continuous integration directly with bank's MDM solutions to ensure that client certificates are replaced before they expire when the employee is in good standing.

CHALLENGE 4:

WE NEED TO AUTOMATE CERTIFICATE ENROLLMENT ACROSS ALL OUR INFRASTRUCTURE DEVICES

"We don't have time to get on the horn with professional services every other day. We just need things to work."
– Infrastructure Architect



The infrastructure architect was tired of stating the obvious: No matter what the bank's CLM vendor claimed, the fact was that the vendor's legacy tools didn't work across existing infrastructure without a great deal of jury-rigging from the vendor's professional services team.

"We desperately need tools that natively—and persistently—integrate with all our web servers and load balancers. Our infrastructure is expanding, and we're increasingly using software-based load balancers in the cloud. We don't have time to get on the horn with professional services every other day. We just need things to work," she said.

In particular, the infrastructure team needed a tool that could automate enrollment and management of the TLS certificates being used on these third-party network devices.

"We also need a tool that can make setting up these configurations easy," added the architect. "We're not PKI experts, so please don't put us in the position of having to figure out all the steps to set up autoenrollment on our F5s and how these steps may differ from our AWS or Azure ones. We really can't afford to get even one step wrong because a few minutes of downtime could cost the bank a lot of money."

Tools needed: Enable third-party network devices to seamlessly integrate with existing infrastructure without disruption; deploy TLS autoenrollment and certificate management throughout enterprise infrastructure; supply configuration templates to simplify set-up of third-party device certificate management automations.

CHALLENGE 5:

WHY CAN'T OUR CLM TOOL MAINTAIN CONNECTION TO OUR EXTERNAL CA?

One of the primary reasons the bank chose their current CLM vendor was because it claimed to work with any CA through the use of connectors.

They boasted about having direct integrations with all major CAs, including DigiCert, the bank's preferred CA.

But the infrastructure architect could think of a few times over the last couple of years where the CLM's connectors stopped working. This meant that requests for new certificates didn't get processed—slowing down projects and increasing the risk of an outage. Sometimes, the vendor took so long to identify the issues with their connectors that the architect instead contacted DigiCert for help. "It's so much easier to call DigiCert because they know PKI better than anyone," the architect said.

After the latest incident, the bank's CLM vendor suggested that the bank should consider migrating their extrernal certificates to another CA, but the architect immediately rejected the idea. After all, if the vendor's CLM wasn't tightly coupled to any external CA, the bank would face the same problem. Meanwhile, the bank had been a DigiCert CA customer for close to two decades, and they could always trust DigiCert to help them no matter the situation. "Our lives would be so much easier if we could just depend on our CLM to work with our external CA," the infrastructure architect mused. "It shouldn't be that hard, should it?"

Tools needed: Provide persistent connection with external CA; deploy TLS autoenrollment and certificate management throughout enterprise infrastructure.

"It's so much easier to call DigiCert because they know PKI better than anyone."
– Infrastructure Architect

CHALLENGE 6:

WE NEED A NEW INTERNAL PKI, PERIOD

The senior PKI administrator was ready to quit. The bank's infrastructure was littered with Microsoft CAs. The PKI team couldn't pinpoint their number, let alone an inventory of keys and certificates that had been issued from them. Her team had found a few orphaned Microsoft CAs, stood up by people who hadn't worked for the bank in years.

Even if they could find every Microsoft CA instance, the human and financial resources needed to continually patch and update them weren't sustainable. Meanwhile, the bank had already failed an internal audit—which portended the likelihood that they would fail their compliance audits. "The level of complexity in staying compliant is off the charts. We need an internal PKI that works across our entire IT infrastructure, including in the cloud—and free us of this chaos," said the PKI admin.

The bank's current CLM vendor mentioned they offered an internal PKI solution that would be able to rip out the old tangle of Microsoft CAs and replace it with a cloud-based solution, but the PKI admin was skeptical. "I did some research, and it's a white label solution that they're sticking their name on. I don't trust it. We need a single-vendor solution," she said.

Tools needed: Rip and replace legacy internal PKI with a standardized internal PKI that works across the enterprise; provide the same level of trust as the bank's external CA DigiCert; gain a unified view across public and private trust resources.

CONCLUSION:

ISN'T IT TIME YOU REPLACED YOUR CURRENT CLM TOOLS FOR A COMPREHENSIVE PKI PLATFORM?

Fortunately, the PKI admin had learned that DigiCert, the bank's primary CA, now offered a managed PKI and CLM solution. During her research, she saw that the solution, DigiCert Trust Lifecycle Manager, provided users with a unified view across public and internal PKI, as well as the ability to set up private roots, spin up ICAs—and automate these processes. "DigiCert has the PKI expertise we absolutely need. Now that DigiCert has an enterprise CLM solution that supports public and internal PKI use cases, I'd say we should be ripping and replacing more than just our private CAs."

After seeing the limitations of their legacy CLM tool, the bank decided it was time to embrace a truly modern digital trust solution that could consolidate all their PKI and CLM requirements under a single platform. DigiCert Trust Lifecycle Manager is not just a CLM solution that can discover, manage, and automate all your x.509 certificates. It's a complete enterprise trust solution that enables you to realize the security advantages that PKI has promised without the complexities that make it difficult to work with or maintain. Isn't it time you ditched your outdated CLM tools for a solution that does everything you need it to do?

Get started today with DigiCert® Trust Lifecycle Manager by contacting us here.