KEYFACTOR

10 things you should know about Microsoft PKI

Microsoft PKI – aka Active Directory Certificate Services (AD CS) – was once an easy choice for IT and security teams. It’s “free,” it’s built into Windows Server, and it’s relatively easy to set up. But the glory days of AD CS are numbered. Let’s explore why.

HERE ARE 10 COMMON REASONS WHY COMPANIES ARE MOVING AWAY FROM MICROSOFT PKI

↓

01

AD CS isn't a big fan of change.

AD CS is overdue for a glow up – sadly, it hasn't seen a significant update since Windows Server 2012. Fast forward to Windows Server 2022, and AD CS remains largely feature-frozen. Navigating documentation can feel a bit like archaeology for those new to PKI, sifting through dead links, ancient blogs, and archived articles to find the guidance they're looking for. Unsurprisingly, many turn to Reddit for help.

> **Microsoft CA or just certificates in general, how to set it up, things to look out for. I'm struggling to find guides that have 'this is why we do it this way' in addition to just what buttons to push.**

02

AD CS is easy to misconfigure...like, really easy.

AD CS isn't inherently insecure, but it's got a knack for misconfigurations. Think of it as a Rubik's Cube – a bit too easy to mix up. Bad actors have a field day exploiting AD CS missteps, issuing fraudulent certificates, and elevating user privileges faster than you can say "domain administrator". Even top-notch AD CS setups can fall victim to configuration drift and the occasional user oopsie over time.

"INSECURE ACTIVE DIRECTORY CERTIFICATE SERVICES" was listed in Top 10 Cybersecurity Misconfigurations in a Joint Cybersecurity Advisory by the NSA and CISA.

03

AD CS likes the server closet, not the cloud.

IT leaders are pushing for the cloud, but AD CS isn't ready to leave the nest. Tied at the hip to Active Directory, it falls short on key cloud essentials – containerization, active-active architecture for high availability, infrastructure automation, and support for modern protocols and authentication methods. It becomes near impossible for teams to meet new demands without making operational or security compromises.

> **Organizations say flexible deployment is the most important feature when evaluating PKI solutions.**
>
> – 2023 State of Machine Identity Management.

> **DCOM is a great technology for what it was designed for but unfortunately that design did not include the internet or firewalls.**
>
> – Unmitigated Risk

04

AD CS isn't exactly firewall friendly.

Setting up AD CS typically requires swinging open a wide range of network ports to support RPC/DCOM, as well as Kerberos and LDAP. There's also no clean separation of certificate authority and registration authority, so issuing CAs must be exposed to all clients on the network. In traditional IT, it can be a firewall management headache. In a hybrid or multi-cloud environment, it's downright impractical and risk-prone.

05

AD CS doesn’t speak DevOps or IoT.

AD CS works well in the Microsoft world, but the buck stops there. Auto-enrollment and SCEP work, but they have their limits. AD CS doesn’t support modern protocols like ACME, EST, and CMPv2, and it definitely missed out on the REST API party. Without these interfaces, AD CS just isn’t well-equipped to support new short-lived TLS certificates, lightweight IoT and network devices, and popular DevOps tools.

57%

of organizations say their existing PKI is incapable of supporting new applications.

– 2022 Global PKI and IoT Trends Study

06

AD CS needs more than a little TLC.

AD CS gives you an engine, a steering wheel, and four tires – necessary to hit the road, but not enough on their own. To bridge the gap, many teams “DIY it” with custom scripts, spreadsheets, and in-house concoctions to supplement their PKI. Unfortunately, these can make administration more complex, inefficient, and fragile over time. Manual configuration, a lack of centralized management across multiple CAs, and limited reporting just leave too much room for error and oversights.

41%

of organizations still use spreadsheets to track certificates.

– 2023 State of Machine Identity Management.

07

AD CS can get complex (and costly) at scale.

PKI operators shouldn't have to moonlight as Windows Server jugglers or AD aficionados. AD CS confines organizations to a single CA per server, creating a scenario where PKI administrators have to deploy another VM and server license every time they need to add a CA for a new use case. In many cases, they wind up with an unnecessarily large number of servers, all of which need to be hardened, managed, updated, maintained, and ultimately, paid for.

58%

of organizations say reducing complexity in their PKI infrastructure is a top priority.

– 2023 State of Machine Identity Management.

256k

Organizations have an average of 256,000 internally-issued certificates.

– 2023 State of Machine Identity Management.

08

AD CS has its limits.

In larger deployments with high volumes of certificates, AD CS starts to show its age. Database queries can become sluggish and operations begin to slow. If you need to reboot the system or restart the CA, it can sometimes take 15 to 30 minutes or more to fully restore services. The database also can't be shared between CAs, making it tough to handle high certificate volumes efficiently.

09

AD CS isn't ready for the next frontier.

Moving from SHA-1 to SHA-2 left organizations with battle scars, and the leap to post-quantum algorithms promises a whole new level of complexity. Currently, AD CS has no clear path to quantum-readiness and doesn't support newer algorithms like EdDSA or new use cases like SSH, Matter, and V2X. For companies with tight security and use case requirements, AD CS just isn't the right fit.

48%

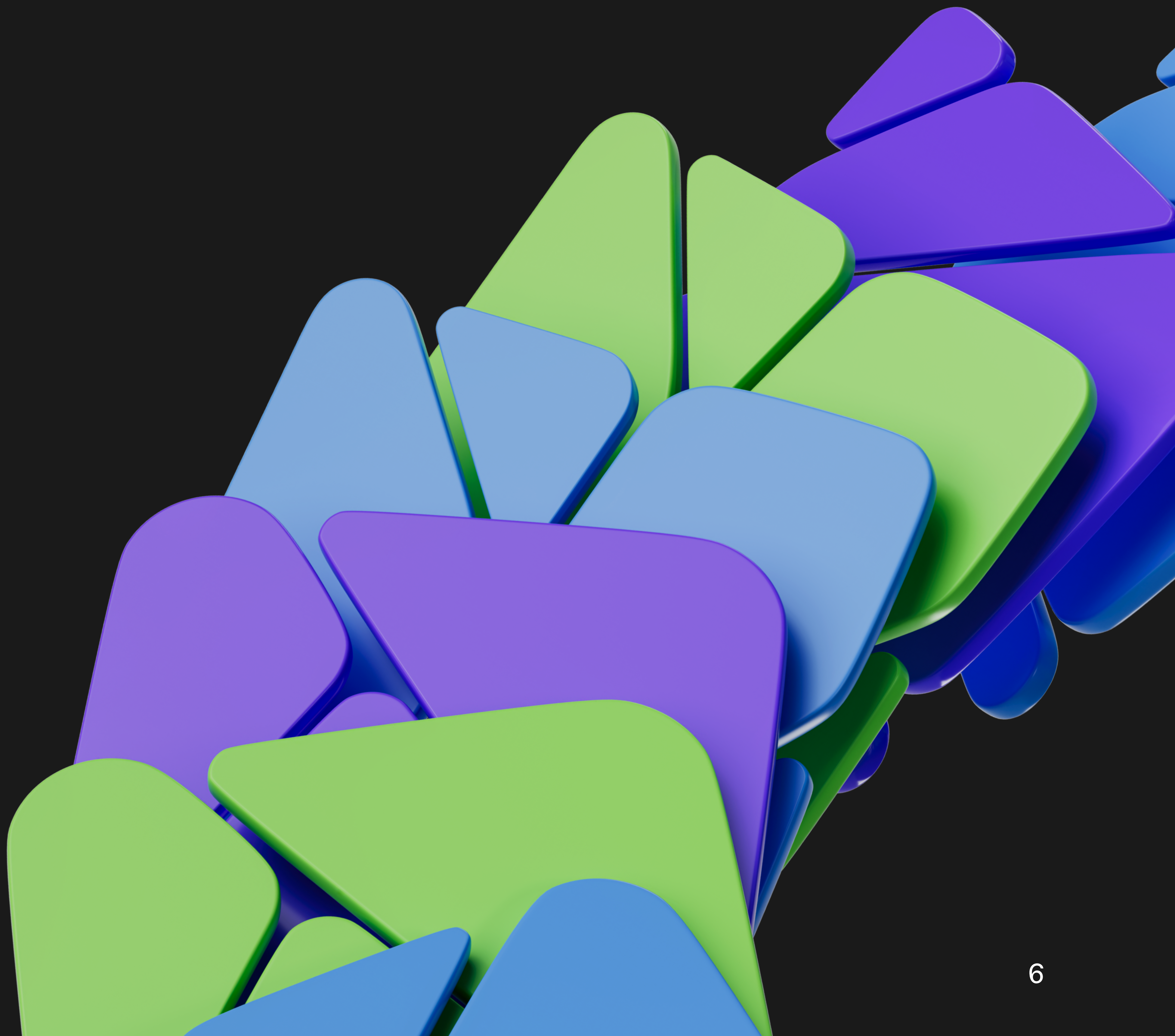
of organizations are concerned about the ability to adapt to changes in cryptography.

– 2023 State of Machine Identity Management.

10

AD CS doesn't have a clear future.

As Azure takes center stage, AD CS doesn't align with most organizations' strategic priorities. While not officially sunsetted, Microsoft continues to push customers from AD to Entra ID, which lacks an AD CS alternative. As organizations make the shift to Azure and other cloud services, the cost of supporting AD CS increases over time as the rest of the ecosystem evolves out of compatibility.



It might be time to say goodbye to Microsoft PKI.

AD CS has been a trusty, but cumbersome, sidekick to deploy and manage. Now, it’s just cumbersome. New use cases, cloud migration, and changes in the security landscape call for a new approach. Modern PKI alternatives have emerged, providing more flexibility, scalability, and automation to better support new requirements. Migration might sound daunting, but it’s easier than you think.

KEYFACTOR

Talk to us about migrating to a modern PKI with EJBCA

Contact us

Not ready to talk? Explore the difference between Microsoft PKI vs EJBCA

Explore