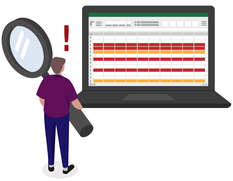
5 Steps to Scale and Automate Certificate Management

The exponential growth in certificate usage, shorter lifecycles, and new DevOps and IoT use cases have changed the PKI game. Here's a quick tool to assess where your certificate management maturity stands — and where you need to be.

LEVEL 1 • MANUAL

Spreadsheets & Scripts

At Level 1, you're using a spreadsheet or database to keep track of certificates, and some form of scripting or emails to notify users about expirations. If you're stuck here, you've probably learned the hard way that it just isn't scalable.



Five Reasons to Ditch the Spreadsheets

01 Spreadsheets only account for known certificates

02 Keeping track of locations, owners and expiry is hard

03 It's also time-consuming and prone to error

04 Custom scripts are rigid and difficult to maintain

05 Certificate requests are still a slow, manual process

100+

It typically takes at least one full-time equivalent (FTE) to manually track and manage 100 or more certificates.[1]

LEVEL 2 • SILOED

CA-Provided Tools

At Level 2, your team needs more oversight into certificate issuance and usage. It's easy to turn to tools offered by your SSL/TLS vendor, but each tool only manages certificates issued by their own CA and doesn't provide insight into where certificates are installed.

The Problem with Manual & Siloed Approaches

Organizations now use an average of eight separate issuing CAs for internal and external certificates.[2]

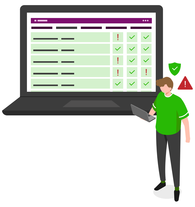
73% of businesses still experience outages due to expired or misconfigured certificates in their network.[3]

Clients typically discover 5-10 times more certificates in their environment than they expected.[4]

LEVEL 3 • REACTIVE

Complete Oversight

Up to this point, you were using disparate tools and processes. At Level 3, you make the decision to adopt a tool that can discover and bring all certificates into a single inventory. Now you can monitor status, build reports, and set expiration alerts for app owners.



3-6 hours

It takes three to six hours to manually request, issue install, and validate a certificate on a server.[5]

You're not out of the woods yet...

Now you have complete visibility, but you're still stuck in a "reactive" mode. Certificate requests and renewals require hours of repetitive work, which only multiplies with more certificates and shorter lifecycles.

LEVEL 4 • PROACTIVE

Lifecycle Automation

At Level 4, automation takes center stage. It's time to take back hours spent on manual certificate requests and renewals. Now you give users a one-stop shop to self-service certificate requests and automate renewals and provisioning – no intervention needed.

Taking it to the Next Level

CLOUD-FIRST PKI

62% of organizations have already or are planning to move their PKI to the cloud.[6]

DEVOPS

More than 50% are using certificates to secure containers and microservices.[7]

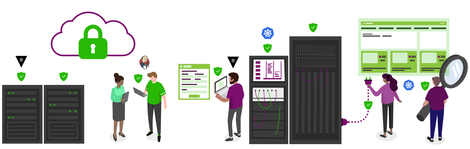
CRYPTO-AGILITY

Only 30% are confident they can respond effectively to algorithm compromise.[8]

LEVEL 5 • DYNAMIC

Crypto-Agility

If you've reached Level 5, you're at premier status. Now you're able to integrate security-approved PKI with automated DevOps tools and IoT initiatives. Not only that, you also have processes in place to stay agile and respond quickly if a CA or algorithm is compromised.



KEYFACTOR

Keyfactor empowers enterprises of all sizes to escape the impact that breaches, outages and failed audits from mismanaged digital certificates and keys have on brand loyalty and the bottom line. Powered by an award-winning PKI as-a-service platform for certificate lifecycle automation and IoT device security; IT, InfoSec, and DevOps teams can easily manage digital certificates and keys. And product teams can build IoT devices with crypto-agility and at massive scale. Exceptional products and a white-glove customer experience for its 500+ global customers have earned Keyfactor a 98.5% retention rate and a 99% support satisfaction rate.

CONTACT US

▶ www.keyfactor.com

▶ +1.216.785.2990

SOURCES

[1, 4, 5] Technology Insights for X.509 Certificate Management, David Mahdi, David Collinson, October 3, 2019

[2, 3, 7, 8] 2020 Keyfactor-Ponemon Institute Report, The Impact of Unsecured Digital Identities

[6] 2019 Global PKI and IoT Trends Study, NCipher and Ponemon Institute