Keyfactor Tech Days 2023

20+ Years of Keyfactor and PrimeKey

How can lessons from the past help with our PKI future?

Ted Shorter

Chief Technology Officer

Keyfactor

20 Years is a Long Time…

...but PKI has come a long way

Russ Housley
Founder
Vigil Security, LLC

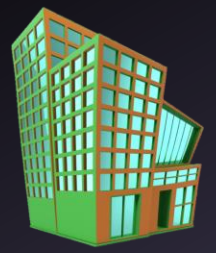
David Hook
VP Crypto Workshop
Keyfactor

Evolution of PKI: The First Wave

1995 - 2002: Beginnings of PKI

- Nearly all digital certificates in use are purchased from public vendors (SSL / TLS)
- Government PKI emerges
- Most organizations have only a handful of certificates
- Large-enterprise PKI: lots of unfulfilled potential

Evolution of PKI: The Second Wave



2003 - 2010: The Enterprise PKI Emerges

Microsoft CA

(Active Directory Certificate Services)

Large organizations issue thousands of certificates (100,000+)

Enterprise Use Cases:

- Authenticating a mobile workforce
- Internal encryption

“Home grown” PKI challenges

PKI and certificate management begins to become a problem

Evolution of PKI: The Third Wave

2011 - Today: New Uses and Growing Pains

Internet of Things

Automation

Organizations' certificates can number in the millions

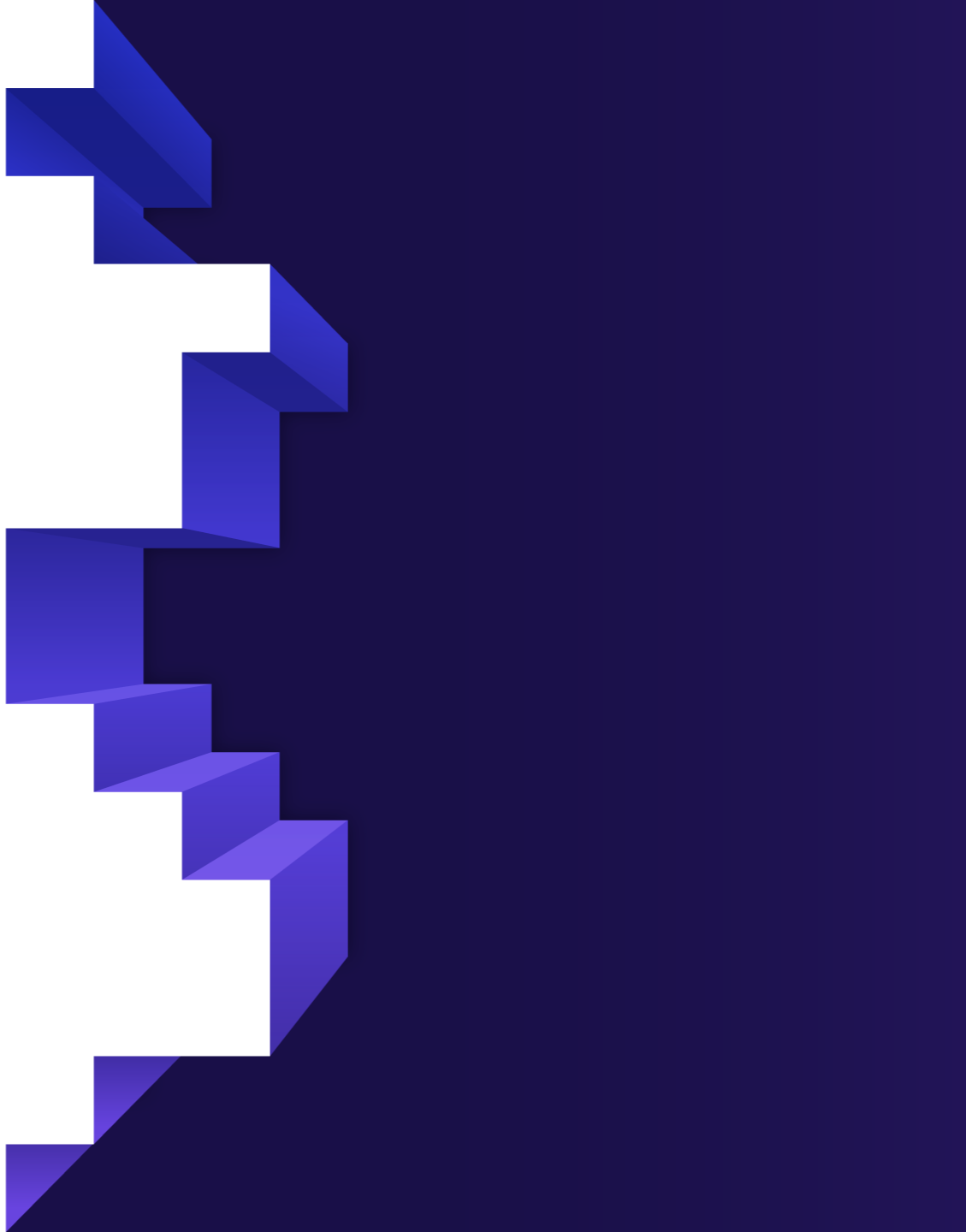
Problems

Oversight at scale / unplanned expirations

Management and update challenges

Achieving "crypto-agility"

What We've Learned



PKI is Hard

Or at least hard to do *well*

Formats and standardization can be a challenge

… but non-cryptographers “just want it to work”

It’s hard to change algorithms

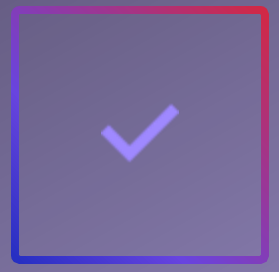
Fun Fact:

As of Jan 24, 2023, there were still ***143 million*** TLS certificates exposed to the Internet with SHA-1 RSA signatures

(source: Censys.io)

RSA key sizes (512, 1024, 2048, 4096…)

MD2 to MD5, MD5 to SHA-1



SHA-1 to SHA-2

Root-of-Trust Management is Important

for functionality,

and security

Automation is a Must

Massive scale is now common and will only increase over time

Algorithmic changeover will likely need to happen more frequently

Let’s Solve This Together

We’ve taken PKI this far…

Smooth PQC migration will take effort from all of us

Thank You!

Ted Shorter, CTO

Keyfactor