KEYFACTOR

WHAT TO WATCH OUT FOR IN

2021

CRYPTO TRENDS REPORT

Preparing for the next wave
of cryptography disruption

FOREWARD

The Next Wave of Cryptography Disruption

Those of us who have worked in cybersecurity for years often think "we've seen it all." We haven't. This year proved that and 2021 will challenge our assumptions again.

Cryptography continues to evolve and expand as a foundational element of enterprise security. Adoption of encryption and authentication has become imperative in 2020, as our organizations were forced to adapt to a new remote workforce, accelerated cloud migration, and the need to secure more data in millions more places.

That said, everything that's considered secure today will be insecure in the future. Algorithms evolve, vulnerabilities arise, and attackers find new ways to abuse the cryptography that underpins security in our organizations.

No business is immune. Consider the steep rise in crypto-related outages that disrupted tech leaders the likes of Spotify and Microsoft, mass certificate revocations, or the growing abuse of code-signing certificates in the gaming industry. No doubt, these trends will continue, and worsen, if cryptographic keys and digital certificates remain widely unmanaged and unprotected.

If there's one key takeaway in this report, it's that there's never been a better time to define a crypto-agility strategy for your organization. The stakes are high, and rising every day as we move closer to a post-quantum reality.

This report highlights the top trends in the crypto-landscape expected in 2021 and beyond, and provides guidance on how to prepare for the next wave of cryptography disruption.

CHRIS HICKMAN
CHIEF SECURITY OFFICER
KEYFACTOR

Table of Contents

INTRODUCTION

Why Cryptography is Critical Infrastructure

Cryptography is everywhere. It's now foundational to everything from operational security like public key infrastructure (PKI) to new ventures like DevOps and the IoT. It underpins actions we take all the time, including bank transactions, streaming videos and even securing passports.

As a result of this ubiquitous nature, cryptography is critically important to modern businesses. And this importance will only increase, as the use of cryptography is poised to grow exponentially over the next few years, particularly as new use cases around advanced technology continue to emerge.

> "Cryptography is foundational to everything we do, from bank transactions to streaming videos, passwords to everyday life."

JOHN RAY,
DIRECTOR HSM PRODUCT MANAGEMENT,
THALES

With adoption of cryptography already at an all-time high and even more growth to come, crypto-management must become an important area of focus for organizations. The innovations we see on the near horizon will change how we conduct business going forward, pitching us into a cycle in which everything that's secure today will become insecure at some point in the future.

This situation makes it essential to look to the future to anticipate what's coming and respond proactively. Doing so effectively requires a high level of agility to adapt in an efficient and non-disruptive way to your business. It also requires keeping close tabs on emerging trends to identify what changes are imminent.

To that end, let's explore the top five trends in cryptography for 2021 and beyond.

TREND #1: THE RESURGENCE OF PKI

Expanding use in IoT and DevOps Deployments

Over the past year, we've seen rapid expansion in the use of PKI, especially in IoT and DevOps deployments, as a core technology to enable identity and authentication.

> "Organizations end up issuing millions of certificates that may or may not be compliant with corporate policy"

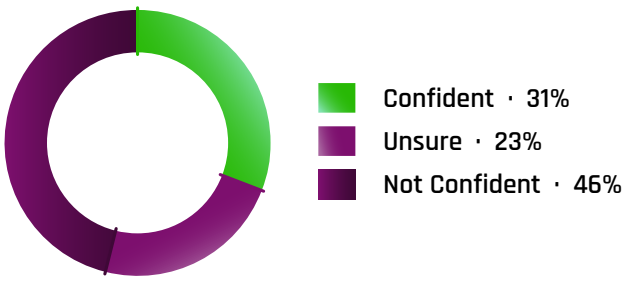
CHRIS HICKMAN,
CSO, KEYFACTOR

PKI IN IOT

Manufacturers need a way to authenticate connected devices and securely update firmware. PKI enables the necessary identification, signing, and encryption to make those activities possible. As the number of IoT devices continues to explode, the use of PKI -- especially a strong root of trust to securely identify and update these devices -- will be critical.

However, IoT manufacturers run into several challenges such as hardware constraints and insufficient PKI expertise, making it difficult to implement properly. For instance, a recent study by Keyfactor found several IoT devices with weak RSA certificates vulnerable to attack. Using high-entropy key generation, maintaining a secure root of trust, and having the ability to update software and keys on devices will be essential to the success of PKI in IoT moving forward.

Confidence in the ability to maintain IoT device identities and cryptography over the device lifecycle:



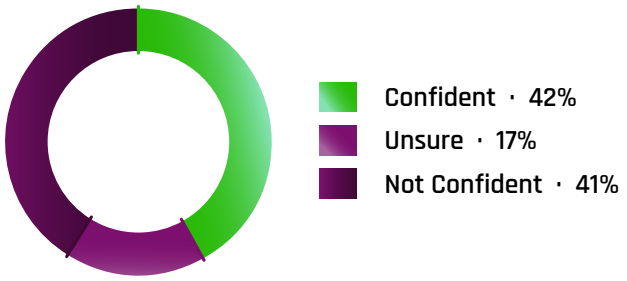
2020 Keyfactor-Ponemon report

PKI IN DEVOPS

The shift left has meant that developers are starting to build security into code during the development phase, including cryptography. Along the way, developers use technology that allows them to generate and issue certificates without any security oversight. While this approach helps maintain a fast pace, it can prove risky from a security standpoint.

Security teams are taking note however, and many have started working more closely with their development teams to ensure compliance. The best way to do so is to align security with development needs by introducing security-driven PKI tools that are easy for developers to adopt and have fully compliant standards for certificate creation built in as the default mode.

Confidence in the ability of PKI to support new initiatives, such as DevOps, Cloud and Zero-Trust strategies:



2020 Keyfactor-Ponemon report

TREND #2: CRYPTO-EXPLOITS

Code Signing, SSH, TLS & CA Compromises

Reports of security breaches and outages due to the misuse of keys and certificates are increasing in frequency. While one reason for this increase is that we are getting better at detecting crypto-exploits, these events are also happening much more often and they show no signs of slowing down, with threats happening at all layers of the stack.

CODE-SIGNING BREACHES

When it comes to application development, risks lie in unprotected code-signing keys, developers accidentally exposing keys in software/firmware, and overall weaknesses in the signing process itself. Failure to protect code-signing keys is an industry-wide problem that attackers will continue to exploit as a method to sign and spread malware.

SSH-BASED ATTACKS

Unlike SSL certificates, SSH keys don't expire. Improper SSH key management creates significant risk of key sprawl as weak, outdated, and unused keys accumulate across enterprise networks. SSH is a natural and growing target for hackers that seek to steal keys or insert their own authorized keys to create persistent backdoor access to systems.

CA & TLS COMPROMISES

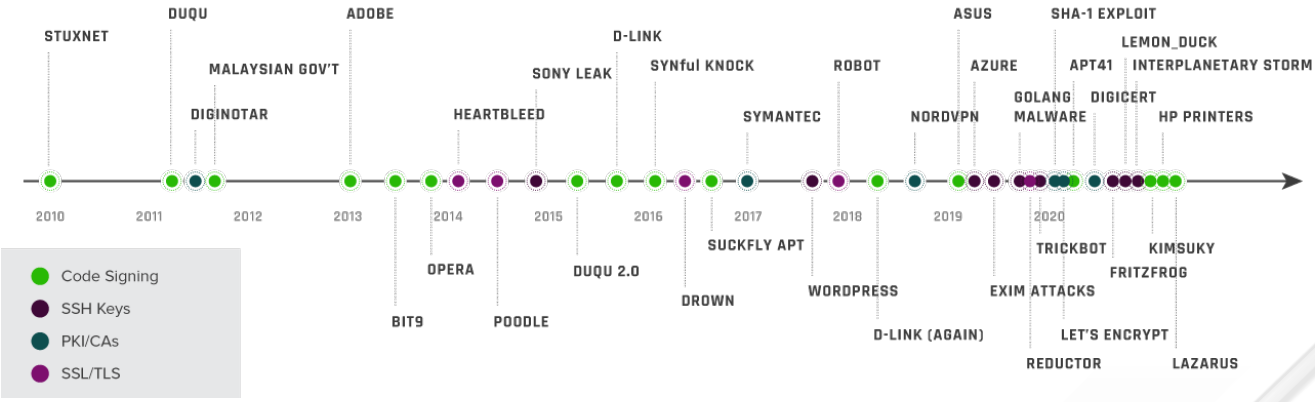
Lack of visibility into the certificate landscape, and the inability to identify and replace weak, rogue or non-compliant certificates, creates an enormous risk for compromise. This leaves organization unprepared to adapt to vulnerabilities and CA-level mishaps, such as the recent mass revocation of 50,000 EV certificates by DigiCert.

> "Threats happen at all layers of the stack; everything from the administration of a system using code signing keys all the way down to the fundamental algorithms being used"

MIKE BROWN
CO-FOUNDER & CTO, ISARA

The biggest takeaway here is that even though organizations are introducing measures to protect data, introducing those measures alone is not enough. Organizations must also invest in managing and protecting keys and certificates, for example by rotating keys and maintaining a clear inventory of all certificates in place and the access they provide, to realize the necessary — and intended — level of security.

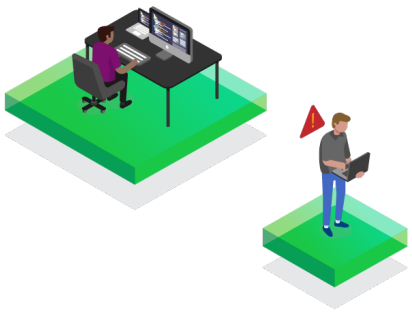
Making these investments to properly protect keys and certificates will shore up these weaknesses and slow down the momentum of crypto-exploits.



KEYFACTOR

KEY TRENDS: THREATS & VULNERABILITIES

A slew of reports in 2020 of malware, vulnerabilities, and attacks involving keys and digital certificates underscore the importance of preventing misuse. Here are a few notable trends we expect to continue into next year.



SOFTWARE SUPPLY CHAIN ATTACKS

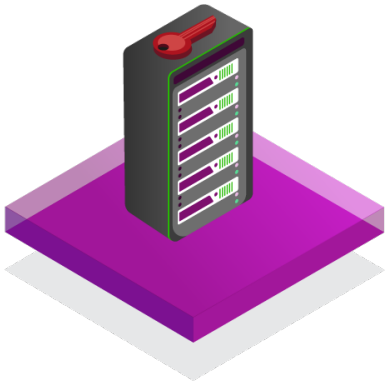
From Stuxnet to ShadowHammer, and recent attacks by APT 41, code signing has proven to be a deeply impactful tactic for attackers in compromising software supply chains. Code-signing vulnerabilities are particularly troubling because, if used successfully, they let attackers impersonate trusted software and bypass defenses.

Consider the dark turn state-sponsored hacking groups took in 2020, using stolen code-signing certificates to sign and distribute malware targeting human rights groups and pharma companies working on COVID-19 therapies.

LINUX MALWARE & SSH ABUSE

Linux is the heartbeat of most data centers and cloud environments today. As a result, malware built to target Linux systems is on the rise. As the de facto standard for remote access, SSH has become a primary attack vector.

More sophisticated SSH-abusing malware variants, such as Lemon_Duck and Fritzfrog, continue to emerge. These attacks use multiple techniques to exploit SSH vulnerabilities, such as brute-forcing SSH password-based logins and injecting backdoor keys.



MACHINE IDENITITES, HUMAN ERROR

As DevOps strategies take hold, security is increasingly under the control of developers. However, developers are not well versed in the risks and proper handling of machine identities (e.g. SSH keys, TLS certificates, encryption keys, etc.). The result is a growing number of misconfigurations and accidental exposures.

For years, developers have been inadvertently publishing sensitive private keys to publicly accessible locations. As recently as January 2020, TLS certificates with private keys were embedded in software and shipped with Netgear devices.

TREND #3: SHORTER TLS CERTIFICATE LIFESPANS

Short-Lived Certificates Will Cause Disruption

As of September 2020, the CA/Browser Forum shortened certificate lifespans to just 13 months (or 398 days). This change came on the heels of numerous other changes over the course of the past decade. In fact, just five years before, the forum moved to shorten the certificate lifespan to 60 months. The intention behind these changes is to increase protection, but each reduction in certificate lifespans has increased the burden of managing certificates and keys.

With the latest change, organizations have one year to renew all SSL certificates from public CA vendors. Budgets and resources remain fixed, but this change essentially doubles workloads and makes managing certificates significantly more complex. The consequence of mismanaged certificates is a highly expensive, highly disruptive outage – not to mention considerable risk.

Over the past few years, the ever-shortening lifespan of certificates has already led to several high profile disruptions, including Equifax in 2017, the US government and Firefox in 2019, and GitHub and California's CalREDIE COVID reporting system in 2020. In these cases, the biggest points of failure have not been public-facing web server certificates, but rather a combination of other certificates that run in the background and are used for client authentication and mutual TLS (mTLS).

Ultimately, while the intention behind these shortening lifespans — to improve security — is a good one, the result is a burden on PKI teams. The best way to deal with this situation is to (1) get a complete inventory of all certificates, where they're installed and when they expire, (2) plan for the renewal of certificates (ideally using automation), and (3) enact a plan to put that process into action and for how to respond should any outages occur.

2012
Lifespans shortened to 60 months (5 years)
CA/Browser forum

37%

2015
Lifespans shortened to 39 months (3 years)
CA/Browser forum

35%

2018
Lifespans shortened to 27 months (825 days)
CA/Browser forum

Google proposes one-year lifespans
2019

51%

2020
Apple limits lifespans in its ecosystem to <398 days

SEPT 1
Lifespans shortened to 13 months (398 days)
CA/Browser forum

NEWS

Apple strong-arms entire CA industry into one-year certificate lifespans

Apple, Google, and Mozilla reduce the lifespan for HTTPS certificates to 398 days, against the wishes of Certificate Authorities.

ZDNet

TOP 2020 OUTAGES: LESSONS LEARNED

Shortened certificate lifespans came into effect this September, but we'll see the net impact of the change in 2021 when teams suddenly have to manage certificate rollover, especially if they lack automation and tools to support those efforts.

MICROSOFT TEAMS

REPORTED: FEB 2020
EXPIRED: CLIENT CERTIFICATE

Microsoft Teams went down for nearly three hours after they forgot to renew a client authentication certificate. These 'client' certificates are much more prevalent with the adoption of cloud and microservices. However, they're typically a blind spot in most organizations, as legacy certificate management tools focus almost exclusively on server-side certificates.

LESSON LEARNED

Every certificate must be inventoried and managed, not just server certificates.

SPOTIFY

REPORTED: AUG 2020
EXPIRED: WILDCARD CERTIFICATE

Spotify experienced a widespread outage affecting streaming services when a wildcard certificate expired without renewal. Wildcard certificates are a double-edged sword. While convenient, without proper visibility and lifecycle management, it can be difficult to find and replace the certificate across all the locations it's been installed.

LESSON LEARNED

Use of wildcard certificates should be limited and tightly controlled.

GITHUB

REPORTED: NOV 2020
EXPIRED: SSL CERTIFICATE

An SSL certificate expired on GitHub's content delivery network (CDN), leaving users unable to access images and JavaScript files. While the outage lasted for just 30 minutes before GitHub managed to acquire and install a new certificate, users immediately took to Twitter and other social channels to express their frustration.

LESSON LEARNED

Even 30 minutes of partial downtime can cause widespread user frustration.

TREND #4: IMPENDING ROOT CA EXPIRATIONS

A "Sleeping Dragon" Behind Your PKI

One of the most predictable, yet under-recognized trends on this list is the impending doom of root CA expirations. As root CAs expire, any certificates that chain up to those roots will no longer be trusted. This situation makes it imperative to monitor root CA expiration and manage root stores on end-devices.

However, monitoring alone won't solve the problem. That's because technologies using these certificates must accept a software update to get the new certificates, and if they can't accept those updates in time -- or, more likely, if their users don't accept updates on the devices – the update fails and the certificate is no longer trusted.

The first signs of trouble emerged this year when the AddTrust CA expired in May 2020, causing widespread outages for streaming and payment services like Roku, Stripe, and Spreedly. Now, products are being designed to manage Roots of Trust out of band to software updates - but that process doesn't extend to legacy products. If you don't update your legacy roots, you can't push updates, resulting in potential device failure.

With multiple root CAs set to expire in 2021 (see below), it's essential to ensure that updates can be sent efficiently and effectively to embedded and non-traditional operating systems, recognizing that many legacy devices may be unable to receive these updates.

Another wrinkle in all of this is UNIX-based systems, as these devices cannot accept certificates with expirations beyond the year 2038. This situation is poised to be a very big problem without a clear solution that has not received much attention to date.

Overall, it's important to recognize that managing a root store is equally as important as managing certificates and that dealing with root CA expirations is not as simple as just updating certificates to a new root. Despite these challenges, the one positive is that these expirations are tied to dates and they are something for which organizations can plan with the appropriate advanced notice.

NEWS

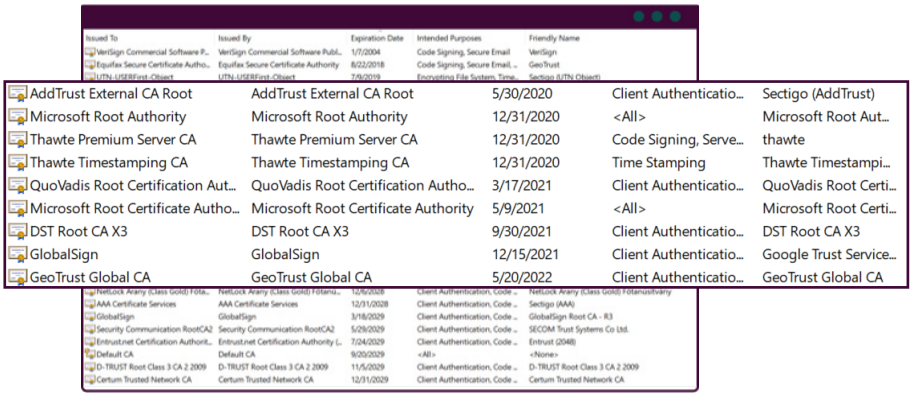
Smart TVs, fridges and light bulbs may stop working next year: Here's why

tom's guide

NEWS

Networked devices will stop working as root certificates expire

DUO



Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Client Authenticatio...	Sectigo (AddTrust)
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>	Microsoft Root Aut...
Thawte Premium Server CA	Thawte Premium Server CA	12/31/2020	Code Signing, Serve...	thawte
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time Stamping	Thawte Timestampi...
QuoVadis Root Certification Aut...	QuoVadis Root Certification Autho...	3/17/2021	Client Authenticatio...	QuoVadis Root Certi...
Microsoft Root Certificate Autho...	Microsoft Root Certificate Authority	5/9/2021	<All>	Microsoft Root Certi...
DST Root CA X3	DST Root CA X3	9/30/2021	Client Authenticatio...	DST Root CA X3
GlobalSign	GlobalSign	12/15/2021	Client Authenticatio...	Google Trust Service...
GeoTrust Global CA	GeoTrust Global CA	5/20/2022	Client Authenticatio...	GeoTrust Global CA

ADDTRUST ROOT CA

On May 30th, the Sectigo (formerly Comodo) Root CA expired

FIRST SIGNS OF TROUBLE

Roku, Stripe, Spreedly and others experienced widespread disruptions

LEGACY DEVICES

Many devices aren't supported long enough to receive updates

UNIX SYSTEMS

All UNIX-based systems cannot accept certificate valid beyond 2038

TREND #5: CRYPTO-POCOLYPSE

Quantum-Safe Cryptography & Evolving Standards

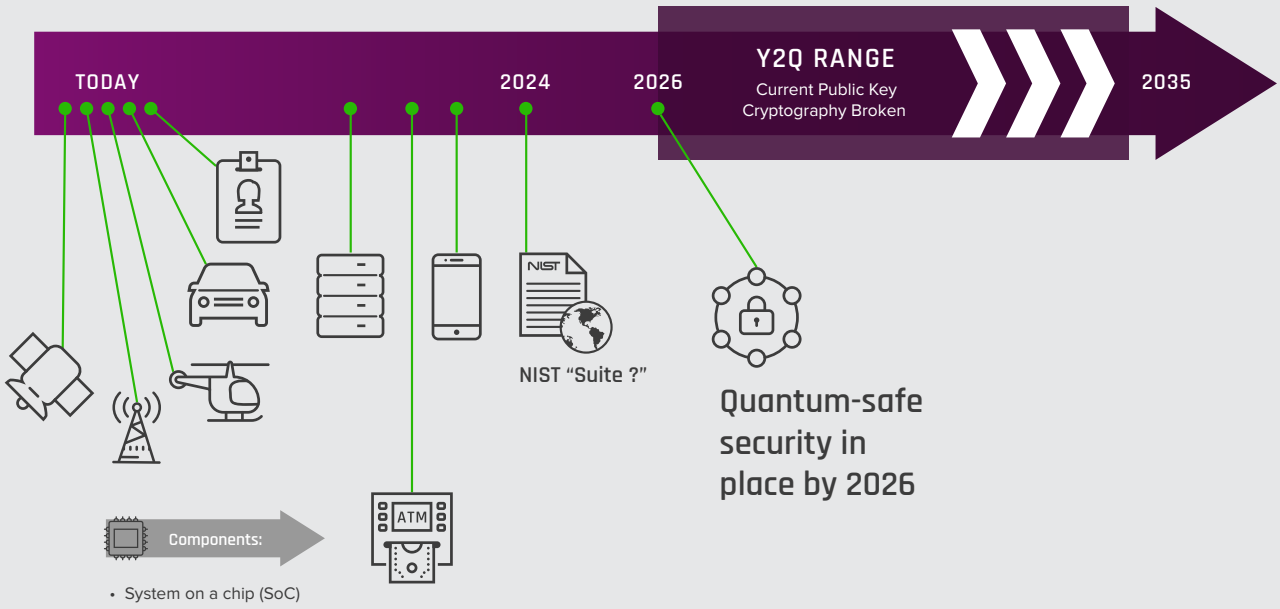
Quantum computing harnesses the unique properties of quantum physics to break barriers currently limiting the speed of today's "classical" computers (as they're now called). In reality, quantum computers will not replace classical computers, but they will be able to solve very specific, complex problems that even the fastest of today's supercomputers can't solve.

While we're still in the early stages of identifying a scalable architecture on which to build quantum computers, these computers will become a reality at some point in the near future. In fact, many companies big and small are making progress toward this future state. And when quantum computing does arrive, it will have an enormous impact on cryptography as we now know it.

Specifically, a large-scale quantum computer will break current public key cryptography, causing widespread vulnerabilities. As a result, we need to start thinking now about how we protect ourselves by making proactive changes to introduce a public key cryptography that's safe against quantum computers. We've already made strides in this area, for example with evolving standards from NIST, but this work must continue going forward.

This change will need to occur on a large scale and it will take a while, so it's something organizations must already start thinking about and planning for so as not to get caught off guard. Draft standards for Post-Quantum Cryptography (PQC) are expected from NIST by 2022-24, but while the world waits for the standards to be finalized, the issue of how these new PQC will be deployed at scale is an exercise that needs to start today as deployment will take years.

WHO SHOULD PREPARE NOW?



–

Image: https://securityboulevard.com/2020/09/adopting-quantum-cryptography-why-y2q-will-be-too-late/

WHAT'S NEEDED:

Crypto-Agility

We expect a lot of changes in the cryptography landscape in 2021, but all of these changes have one thing in common: they can be planned for ahead of time.

It's easy and attractive to look at big bang moments, such as quantum advancement, but there are a lot of little things that happen every day in the lead up to those moments, and how organizations handle those transitions is critical to success.

Given the changes on the horizon, the top priority for organizations going forward should be to define policies and priorities for crypto-agility. Specifically, crypto-agility centers around three key areas:

> "By 2021, organizations with crypto-agility plans in place will suffer 60% fewer cryptographically related security breaches and application failures than organizations without a plan."
>
> GARTNER, BETTER SAFE THAN SORRY: PREPARING FOR CRYPTO-AGILITY, MARK HORVATH, DAVID ANTHONY MAHDI, 6 AUGUST 2019

PLANNING:

Knowing which devices and apps are dependent on cryptography; identifying keys, certificates, algorithms and crypto-libraries in use; and prioritizing assets and assigning teams to them before a crisis.

INVENTORY:

Planning for obsolescence of algorithms and crypto-libraries; understanding options for replacements; and determining which algorithms will and will not be suitable.

RESPONSE:

Extending incident response plans to crypto-agility; testing transition plans and mechanisms; and asking third party vendors about their transition plans.

BOTTOM LINE

The time to start focusing on crypto-agility is now. Doing so will prepare your organization to handle both expected and unexpected changes while sidestepping negative outcomes like outages and crypto-exploits now commonplace in many organizations.

Next Steps

Sudden and unpredictable disruptions in the cryptographic landscape can leave your organization exposed to serious risk and disruption to productivity.

Keyfactor is the industry leader in crypto-agility solutions. We provide teams with the tools they need to deploy, manage, and automate keys and digital certificates across their business.

Ready to enable crypto-agility in your enterprise? See our products in action now.

See a Demo ▶

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 and InfoSec 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.

Learn more at **keyfactor.com**

CONTACT US

- www.keyfactor.com
- +1.216.785.2990