# PKI Checklist for Business Continuity

## HOW TO SCALE & SECURE YOUR PKI IN UNCERTAIN TIMES

Every year, enterprises face unforeseen events that can disrupt operations. These events are rarely predictable, and they often create significant challenges for IT and security teams, the network, even hardware supply chains. That's where business continuity comes in – to ensure that core functions remain intact, despite the disruption. A critical component of business continuity is public key infrastructure.

PKI is at the core of enterprise IT. It's a fundamental tool used to protect sensitive data and secure connections across multiple business-critical applications. In fact, the average PKI today supports more than eight different applications[1], from customer-facing websites and services to private network and VPN access. If PKI is mishandled, though, it can create significant disruption and application downtime.

Business continuity planning must account for your PKI and all applications that depend on it. With increasing pressure on PKI to protect new use cases, such as cloud services, mobile and remote workforces, the ability to support scale, availability, and assurance is even more critical.

## Here are 10 Key Considerations to Ensure Business Continuity for Your PKI:

### 01. AVOID A "NEXT, NEXT, NEXT" PKI DEPLOYMENT

If you're standing up a new CA to expand certificate use cases (e.g. SSL VPN) or meet a rapid increase in certificate issuance, resist the temptation to cut corners during implementation. Sometimes it's just too easy to click "next, next, next" when configuring a Microsoft CA, but simple missteps can expose your organization to serious risk and service disruptions down the line.

### 02. KNOW WHEN YOUR ROOT/ISSUING CAs EXPIRE

A fundamental rule in PKI is that a certificate cannot have a lifespan beyond the expiration of the CA it was issued from. If your Root CA expires, all certificates issued from it expire. Industry-standard practice is to renew the Root CA after 10 years, and re-key after 20 years. If your Root CA is up for renewal in the next 8-12 months, you'll need to start planning resources appropriately.

### 03. PLAN FOR PHYSICAL ACCESS TO YOUR ROOT CA

A Root CA is the foundation of trust for your PKI. It should be kept offline, air-gapped from the network, and protected with an HSM. However, this means that routine maintenance tasks like publishing a certificate revocation list (CRL) require multiple staff to be physically present. If remote HSM cardholders are miles (not steps) from the Root CA server, this becomes much more difficult.

### 04. DON'T FORGET ABOUT CRL RENEWAL

If a CA is down, you'll be unable to issue new certificates, but if your CRL is expired, all of your certificates become immediately unusable. That's because most applications need to check the validity of certificates against a CRL or OCSP server. If they cannot reach the CRL server, or if the CRL itself is expired, users will be unable to access their application.

### 05. LEAVE A SUFFICIENT CRL OVERLAP

There are three points in time that matter when it comes to your CRL: the time you publish it, the time it expires, and the period of overlap in between. Remember that CRL publishing is a manual process for offline CAs. The purpose of this overlap is to provide time to manually push the new CRL before the old CRL expires, and to avoid a gap in availability.

### 06. MAKE SURE YOUR CDPs ARE INTERNET-ROUTABLE

When an application checks for revoked certificates, it retrieves the current CRL from a specified CRL distribution point (CDP). After the CRL is retrieved, it's typically cached until it expires. If users move outside your network, the CDP must be reachable over the Internet to ensure that devices can still retrieve the new CRL when needed. The CRL should be accessible via an HTTP URL.

### 07. CHECK THE DISK SPACE ON YOUR ISSUING CAs

It seems simple, but we see issues here far too often. Carefully consider if there is enough disk space on all of the Issuing CA servers to handle expanded use. For example, if you enable thousands of remote workers with certificates for SSL VPN, you must ensure the CA database is equipped to store the influx of certificates and audit logs without latency issues.

### 08. ENSURE THAT YOUR ENTIRE PKI IS REGULARLY BACKED UP

Many assume that, if they have a backup, they can recover their PKI. However, CA backups aren't foolproof and they need to be regularly tested. If you have a backup of your CA database, but not the HSM, the CA can't be recovered anyways. Ensure that everything is automatically and periodically backed up to ensure resiliency should a system failure occur.

### 09. GET A COMPLETE INVENTORY OF YOUR CERTIFICATES

Beyond the nuts and bolts of PKI, it's critical to keep a complete inventory of every certificate issued form both your internal and public CAs. Know where every certificate lives and which applications are dependent on them. If SSL VPN becomes a business-critical application for your workforce, you'll need to re-assess the risk related to these certificates.

### 10. ACTIVELY TRACK WHEN CERTIFICATES EXPIRE AND WHO OWNS THEM

Organizations cannot afford the application downtime or service disruptions caused by expired certificates. However, chasing down application owners to renew their certificates can be challenging if employees work remote. As you build your inventory, actively monitor certificates, define clear responsibilities, and notify owners well before expiration (90/60/30 days).

[1] https://www.ncipher.com/2019/pki-iot-trends-study

© 2020 Keyfactor, Inc. All Rights Reserved | www.keyfactor.com

# Additional Resources

WHITE PAPER

## PKI: The New Best Practices

In this white paper, you'll learn about:

- How today's digital transformation has caused security gaps
- PKI then & now - A look back at previous best practices
- Top 6 PKI best practices - Keys to success for your team
- Build or Buy? In-house PKI vs. PKI as-a-Service

READ THE WHITE PAPER

EBOOK

## 5 PKI Mistakes to Avoid

In this eBook you'll learn:

- About the most painful and costly mistakes commonly seen in PKI deployments today
- Why proper planning and design are critical to preventing a security breach or service outage
- How to avoid the risks and complexities of deploying and running your PKI with PKI as-a-Service

READ THE EBOOK

KEYFACTOR PKI SOLUTIONS WWW.KEYFACTOR.COM

▶ LIVE Q&A

Securing Your New Remote Workforce:
Your Questions Answered from PKI Experts

Chris Hickman
CSO, KEYFACTOR

Mark B. Cooper
PRESIDENT, PKI SOLUTIONS

Ted Shorter
CTO, KEYFACTOR

Q&A DISCUSSION

## PKI Experts on Securing Your New Remote Workforce

Get answers to important questions about how PKI fits into your COVID-19 response in this 30-minute panel discussion with Keyfactor's CSO and CTO, and special guest Mark Cooper

LISTEN TO THE PKI EXPERTS

How can you build and manage your PKI for business continuity?
Connect with one of our PKI experts to learn more.

CONTACT US

KEYFACTOR

Keyfactor empowers enterprises of all sizes to prevent the breaches, outages and failed audits from digital certificates and keys that impact your brand loyalty and bottom line. Powered by the industry's only PKI as-a-service platform, 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.

▶ www.keyfactor.com
▶ +1.216.785.2990

© 2020 Keyfactor, Inc. All Rights Reserved