KEYFACTOR

EBOOK

The Dark Side of Digital Trust

Become a PKI Jedi and Safeguard Your Business Against Evolving Threats to Digital Trust

Table of contents

DISCLAIMER:

We've sprinkled in some galactic references to keep things interesting (because let's face it, even security teams need a little excitement). George Lucas, please don't send the Stormtroopers. May the Force of fair use be with us!

So, you want to be a PKI Jedi?

Patience, PKI padawan. You may even be thinking, “I’m already a PKI master.” Even those trained in the ancient art of public key infrastructure (PKI) must stay vigilant in the ever-evolving digital landscape. The dark side of digital trust never rests — new risks and threats emerge daily. So, whether you’re a PKI padawan or a master, let’s begin your training to defend the future of digital trust.

Digital trust: The good, the bad, and the dark

Welcome to the age of always on. From remote work to smart appliances, more and more of what we use and interact with every day is network- or internet-connected. Connectivity is so pervasive that we barely think about it. But behind every connection, there’s a complex system of trust that makes it all possible.

Digital trust isn’t a theoretical concept; it’s a real-world system of standards bodies, policies, software, and infrastructure that secures interactions between anything and anyone. At the heart of this system is public key infrastructure (PKI), a vital technology that delivers authentication, encryption, and data integrity; it’s a powerful force that ensures our websites and apps work, our payments are secure, and the software we build and consume is safe — a shield against the dark side of the digital realm.

But what happens when trust is undermined, compromised, or even weaponized?

In this guide, we’ll venture to the dark side of digital trust to discover what happens when trust is misused, or worse, wielded and corrupted by malicious actors. We’ll look at real-world threats, security incidents, and outages to understand why they happen and how to defend your business against them.

Unexpected Outages:

Certificates Strike Back

TLS certificates are essential for encrypting data and authenticating connections behind modern IT infrastructure. However, just a single expired or misconfigured certificate can quickly cause system failures and disrupt essential services, often catching IT teams off guard like the Galactic Empire's sudden attacks.

Many organizations try to manage certificates with a combination of spreadsheets, PKI tools, CA interfaces, and custom scripts. While well-intentioned, these methods quickly become problematic as the number of certificates increases. Manual processes can't keep up, leading to missed renewals, increased risk of outages, and potential vulnerabilities.

Recent Incidents:

A root certificate expired behind a major ITSM platform, disrupting operations for over 600 customers, with some experiencing a 90-minute delay in linking their cases to the error. source ↗

The Bank of England's CHAPS settlement system went dark for 91 minutes due to an expired certificate, following a previous outage of their RTGS system. source ↗

Expedia's global websites went down over a weekend, initially attributed to "maintenance", but later revealed to be caused by an expired certificate. source ↗

Thousands were affected when a decade-old hardware certificate expired on SD-WAN devices, causing network failures. source ↗

SpaceX's Starlink service experienced a global outage when a ground station certificate expired, disrupting connectivity for users worldwide. source ↗

FAST FACTS

Certificate outages cause an average of

318 minutes of downtime,

from detection to restoration and root cause analysis.

Google intends to reduce the maximum validity of publicly trusted TLS certificates from

398 days to 90 days,

expected in 2025.

In October 2025, Apple proposed a gradual reduction in the maximum validity of publicly-trusted TLS certificates from

398 days to 45 days

by April 17, 2027.

The frequency of TLS certificate renewals will increase five- to ten-fold as a result.

PKI Jedi Guide:

Master the Unknown

- Maintain a centralized inventory of all certificates — not only server-side TLS certificates, but also client certificates, code-signing certificates, and roots of trust.
- Proactively track expiry dates, locations, and ownership across CAs, network endpoints, cloud services, certificate transparency (CT) logs, and certificate stores.
- Wield the power of automated discovery and lifecycle management solutions to reduce risk and streamline renewals and provisioning.

Rogue CAs & Cert Slingers:

The Rogue Ones

The realm of PKI and digital certificates can sometimes be a chaotic place, much like the lawless deserts of Tatooine. Without standardized policies and governance, CAs are spun up with questionable practices and rogue admins become certificate-slinging outlaws, putting misconfigured or self-signed certificates into production environments.

Application owners use their own tools and workarounds to obtain certificates without any security oversight. To make matters worse, security teams often lack permissions or knowledge of how certificates are consumed by servers and applications, making it difficult to address the problem and prevent resulting outages and audit failures.

Common Culprits:

Wildcard certificates offer convenience by securing multiple subdomains with a single certificate, but they introduce significant risks. Much like the Death Star's fatal flaw, they create a single point of failure if the private key is compromised or the certificate expires without notice, exposing all subdomains to a system outage or phishing attacks.

Self-signed certificates may seem harmless but can lead to serious vulnerabilities. Without validation from a trusted CA, there's little oversight into their quantity, locations, ownership, and private key storage. Like rogue Jedi, they lack accountability; they never expire and can't be revoked, making compromised certificates hard to identify and remediate.

FAST FACTS

On average, IT and security professionals estimate they have

7 different PKI and CA tools

in use across their environment.

42%

of organizations say reducing the risk of unknown or self-signed certificates is a top strategic priority

Certificate issuers built into tools like

Kubernetes or HashiCorp Vault are not

CAs — they should be integrated with a trusted and policy-backed PKI.

PKI Jedi Guide:

Rein in the Chaos

- Consult with application and operations teams to understand their needs and use cases.
- Identify and limit the use of self-signed and wildcard certificates across the business.
- Consolidate PKI and CA tools wherever possible to cut infrastructure cost and complexity.
- Bring balance to the Force between speed and security; enable teams with convenient ways to obtain policy-complaint certificates (e.g., REST API, protocols, and integrations).
- Adopt a PKI solution that supports cloud and container-based deployment models.

Code Signing Sabotage:

Attack of the Code

The software supply chain is perhaps the largest unaddressed attack surface lurking within businesses today. In the past several years we've witnessed several high-profile, targeted attacks on software supply chains across the globe. One of the most common attack vectors is code signing abuse, turning a vital security measure into a potential vulnerability.

Code signing as an attack vector is not new. However, the threat landscape has expanded beyond just stolen or leaked keys used to sign and distribute malware disguised as trustworthy. Attackers now breach signing environments and infect code directly, allowing malware to slip past defenses undetected, as if cloaked by the dark side of the Force.

The Dark Side of Signing:

Adversaries stole source code and private code signing keys from AnyDesk, resulting in a 48-hour maintenance window and requiring users to update their software.

source ↗

After ransom demands from the Money Message group went unanswered, they leaked private code signing keys used for 57 products by Micro-Star International (MSI), potentially allowing bypass of Intel Boot Guard.

source ↗

Attackers compromised code signing certificates for GitHub's Atom and Desktop products, prompting the need for users to upgrade any instances of the app signed with the quickly revoked certificate.

source ↗

The extortion group Lapsus$ leaked two code-signing private keys used by NVIDIA for their drivers and executables; researchers discovered malware signed with these certificates within days.

source ↗

FAST FACTS

Researchers analyzed 3 million software downloads and found that

66% of malicious downloads

were signed using a legitimately issued certificate.

Many IT and security professionals report that code-signing keys are

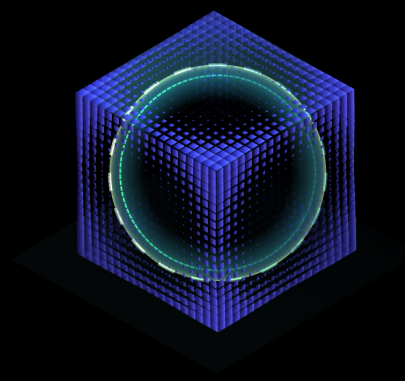
stored on workstations (53%) and build servers (52%)

rather than in secure hardware security modules (HSMs).

As of June 2023, the CA/B Forum mandated that code-signing certificate private keys for public trust usage must be stored in an HSM.

PKI Jedi Guide:

Shield Your Secrets



- Keep your code-signing private keys locked down in a FIPS-compliant HSM.
- Enforce the principle of least privilege through key and signing access controls.
- Automate and integrate secure signing processes into existing tools and workflows.
- Generate a Software Bill of Materials (SBOM) at the time of signing to build confidence in your code through trust and transparency.
- Timestamp your signed code with a proper Time Stamp Authority (TSA).
- Use multi-factor authentication for systems involved in the software supply chain.

Vulnerable SSH Keys:

Revenge of the Myth

Secure Shell (SSH) protocol enables secure administrative access for IT operations like remote logon and file transfer. However, a dangerous myth has taken root: the belief that SSH authentication using passwords or key pairs is inherently secure. This misconception, like a Jedi's overconfidence, leaves organizations vulnerable to corruption.

Akin to a Jedi's lightsaber, SSH keys are powerful tools that require careful handling. When they fall into the wrong hands, they become formidable weapons, allowing attackers to move through systems undetected. Unlike certificates, SSH keys don't expire, they are frequently copied or shared, and often grant excessive privileges.

Common Culprits:

Dormant or forgotten keys created for temporary access or by a former employee are often not removed from systems, leaving them vulnerable to misuse by an attacker.

Weak and hardcoded keys are frequently found in source code or public repositories where they are easily compromised.

Key sharing and forwarding are common bad habits to simplify tasks for IT departments, making it near-impossible to track ownership and access privileges.

Excessive privileges, such as granting unnecessary root access, pose a significant risk of unauthorized internal or external access.

FAST FACTS

SSH key-stealing and brute-forcing malware has been used by attackers for years – from FritzFrog and Lemon_Duck to RapperBot.

In many environments, up to

90% of SSH keys

are unused or unmanaged.

In 2024, Sysdig discovered SSH-Snake, a self-propagating, file-less malware that exploits SSH credentials to spread across networks,

affecting up to 36% of US-based companies.

Remediation requires caution; hastily removing or rotating SSH keys can lead to loss of access and service outages.

PKI Jedi Guide:

Stay Vigilant

- Disable brute-force-vulnerable password-based authentication on all servers.
- Build an inventory of key pairs and map trust relationships between systems and accounts.
- Monitor key attributes like last usage, associated user accounts, key age, and strength.
- Implement key rotation policies and remove hardcoded, dormant, and weak keys.
- Use far more secure and flexible short-lived SSH certificates for authentication.

CA Distrust & Mis-issuance:

The Bad Batch

Not unlike defective clone troopers, sometimes a CA will issue a bad batch of certificates due to a security breach, software bug, or compliance issue. When these incidents occur, hundreds or thousands of certificates are revoked within a very short timeframe to comply with strict industry rules and security standards.

Like a disturbance in the Force, these incidents send shockwaves through the internet, leaving end-user organizations scrambling to identify and replace all affected certificates. In some cases, a CA may even be distrusted entirely by a web browser, resulting in more widespread and long-lasting impacts.

The Bad Batches of 2024:

Entrust announced they would revoke and re-issue more than 24,000 EV TLS certificates that were mis-issued over the previous six months.

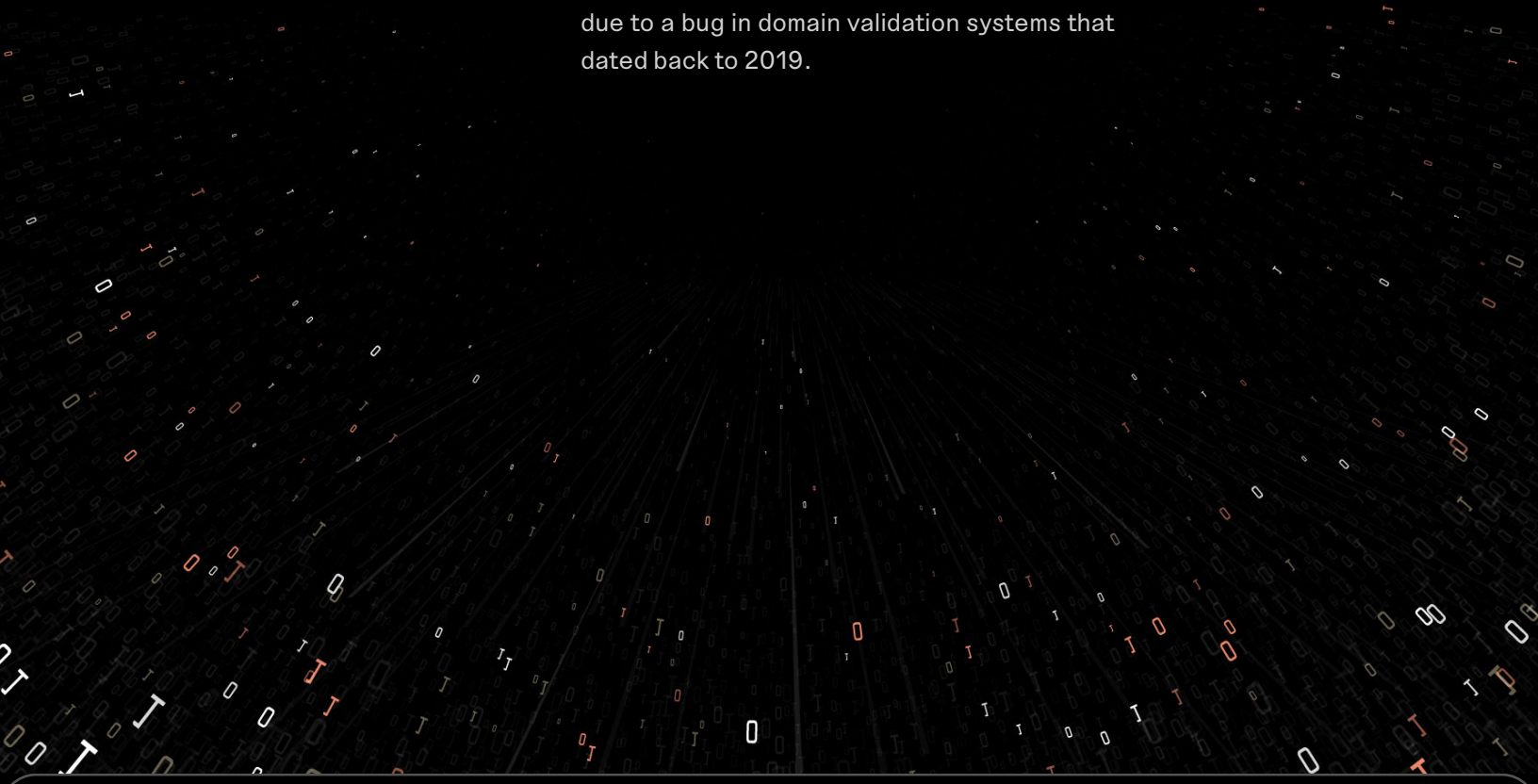
source ↗

Google announced that Chrome would no longer trust TLS certificates issued by Entrust after November 11, 2024, citing a pattern of concerning behavior from Entrust.

source ↗

DigiCert notified 6,807 subscribers they had a 24-hour window to replace affected certificates after 83,627 certificates were revoked due to a bug in domain validation systems that dated back to 2019.

source ↗



FAST FACTS

In 2024, Entrust and DigiCert experienced issues requiring revocation of thousands of certificates — these are not isolated cases, but standard procedure for publicly trusted certificates, and can affect any CA.

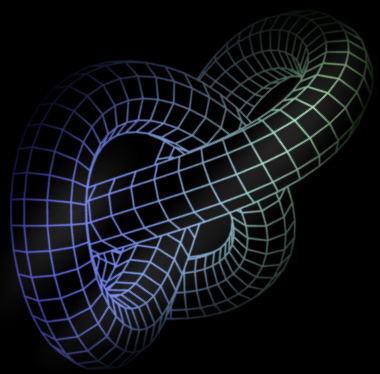
At least 11 CAs have been distrusted

by major web browsers since 2011, including Symantec, Visa, and DigiNotar.

CA/B Forum requires revocation of mis-issued certificates to occur within either 24 hours or 5 days, depending on the nature of the issue.

PKI Jedi Guide:

Adapt with Lightspeed



- Develop and test a plan for rapidly switching CAs in the event of distrust or changes in business operations.
- Avoid CA-lock in; implement a CA-agnostic certificate management solution to ensure complete visibility and control of all certificates.
- Adopt automation to enable renewal and replacement of certificates at scale — ensure that your vendor supports full automation and a wide range of integrations.
- Use private trust certificates from your Enterprise PKI where public trust is not required.

Quantum Computing:

The Quantum Menace

Quantum computers are emerging as a powerful force, promising to revolutionize fields like medicine and climate science. However, like the Force itself, this immense power has a dark side: the potential to break the encryption algorithms we use to safeguard data and communications across the internet.

The quantum threat to cryptography isn't just a future problem; government agencies have warned that malicious actors and nation-states have already adopted "harvest now, decrypt later" attack strategies with the intention of decrypting data once sufficiently powerful quantum computers become available.

Why It's Time to Prepare:

Harvest now, decrypt later attack methods aim to compromise organizations' sensitive data.

The release of new quantum-resilient algorithms signals it's time for security teams to get serious about taking steps to prepare.

Time is not on your side; the transition to post-quantum cryptography is a complex, multi-year process that requires careful planning and expertise.

New mandates and regulations will inevitably emerge as governments and standards bodies aim to drive industry adoption.

FAST FACTS

Gartner predicts that

by 2029,

advances in quantum computing will render applications, data, and networks protected by asymmetric cryptography unsafe.

IBM, a leader in quantum research, believes classical

encryption will be broken within seven to 15 years,

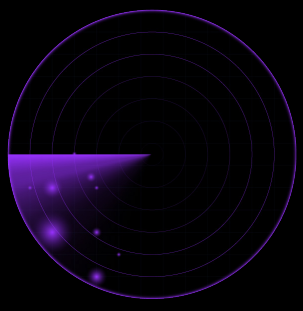
with 10 years being most probable.

More than 70%

of ransomware attacks now involve data exfiltration, where threat actors steal sensitive data before they encrypt the files, indicating this strategy is common

PKI Jedi Guide:

Ready Your Defenses



- Build a comprehensive cryptographic inventory, including keys and digital certificates.
- Talk to your vendors, including your PKI and HSM providers, to ensure they have a roadmap to enable quantum-safe security, now and in the future.
- Develop your migration plan, prioritizing sensitive and mission-critical systems and data.
- Prepare your systems for migration by adopting automated processes, such as automated certificate renewal and provisioning.

Crypto-Agility:

A New Hope for Digital Trust

As dark forces threaten digital trust, crypto-agility emerges as our new hope. Organizations must ready their defenses and evolve their cryptographic strategies to combat real threats — from certificate outages and CA distrust to stealing secrets and sensitive data.

By embracing crypto-agility, security teams can swiftly respond to new vulnerabilities, transition seamlessly to new algorithms, and maintain robust defenses. Crypto-agility is the way, but you need the right tools to achieve it. That's where Keyfactor comes in.

Modernize your PKI

Shift to a fast, flexible, and quantum-ready PKI that deploys on-prem, in the cloud, and as a service.

Keyfactor EJBCA

Embrace agility

Implement a CA-agnostic certificate discovery and lifecycle automation solution to move faster and reduce risk.

Keyfactor Command

Sign with confidence

Enable fast and secure code signing processes with quantum-ready solutions built for developers.

Keyfactor SignServer

So, you're a PKI Jedi.

How about a lightsaber?

As we conclude our journey through the dark side of digital trust, one last piece of PKI Jedi wisdom:

Like a well-maintained lightsaber, certificate lifecycle automation is your most powerful weapon against the forces of chaos.

But how do you convince the Jedi Council (AKA, your executives) to invest in this critical technology? Find your answers in our next eBook, which includes a curated list of questions to ask, making it easy to justify the investment to key stakeholders.

Continue the journey ↗

KEYFACTOR

Keyfactor brings digital trust to the hyper-connected world with identity-first security for every machine and human. By simplifying PKI, automating certificate lifecycle management, and securing every device, workload, and thing, Keyfactor helps organizations move fast to establish digital trust at scale — and then maintain it. In a zero-trust world, every machine needs an identity and every identity must be managed. For more, visit keyfactor.com or follow @keyfactor.

Contact us

- www.keyfactor.com
- +1 216 785 2946 (North America)
- +46 8 735 61 01 (Europe)