



The End of Set-and-Forget PKI: How 47-Day Certificates Change Everything

Reduce your exposure to certificate sprawl, machine identity risk,
and post-quantum timelines.

Contents

Why 47-Day Certificates Change Everything	3
Why Organizations Must Act Now	4
The Hidden Business Risks of Certificate Velocity	5
Machine Identities are Multiplying the Challenge	6
47-Day Certificates as a Foundation for Post-Quantum	7
From Certificate Management to Cryptographic Control	8
Enabling the Shift With a Platform Approach	9
Prepare Now or Pay Later	10

47 Days Changes Everything

Eight renewal cycles per certificate per year, with no margin for missed alerts, manual delays, or process gaps. That’s what a 47-day validity model looks like, and it exposes exactly why the operational models built for annual renewals won’t scale.

Lifecycle Compression Becomes Continuous Operations

An organization managing 1,000 publicly trusted Transport Layer Security (TLS) certificates under a one-year validity model renews each certificate once annually. Under a 47-day model, that same organization manages roughly eight renewal cycles per certificate per year. The result: renewal volumes increase exponentially, and certificate management becomes always-on.

Why Legacy Approaches Fail

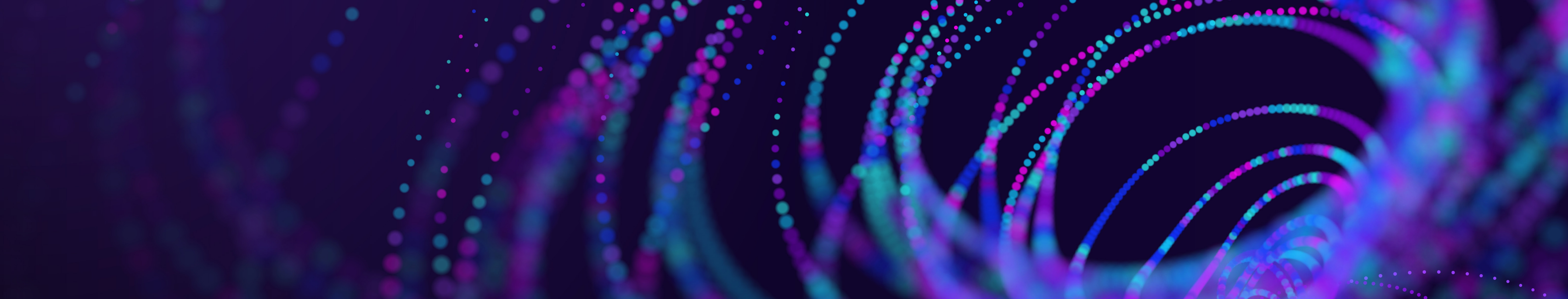
Three structural failures define why the old model breaks:

- **Manual processes can’t scale to high-frequency renewal cadences.** What once only needed to be addressed annually will soon need to happen reliably every few weeks.
- **Siloed ownership creates visibility and accountability gaps.** When PKI and certificate management responsibility is distributed across teams without centralized visibility or policy, coordination delays become outage risks. Approximately 60% of organizations say responsibility for cryptography is fragmented.
- **Processes built for low touch, low volume environments collapse at scale.** Workflows designed to handle dozens of renewals per year simply can’t manage hundreds.

There isn’t a team fast enough, thorough enough, or consistent enough to manage this manually.

From 398 Days to 47:
The Shrinking Certificate Window

Certificate Lifetime	Date	Increase in Operational Burden and Risk
398 Days	Baseline	Baseline
200 Days	March 15, 2026	2x
100 Days	March 15, 2027	4x
47 Days	March 15, 2029	8x



Why Organizations Must Act Now

When certificates fail, the impact is felt immediately.

The mandate is set, but now comes the harder question: Is your organization prepared?

Infrastructure and security teams are feeling the squeeze. The expectations haven't changed but the pressure has: Avoid downtime before it hits the news. Remain perpetually audit-ready. Extend trust at speed for cloud, DevOps, and AI workloads. And limit operational overhead and technical debt that comes from managing certificates as an afterthought.

Public key infrastructure (PKI) has long been treated as “set it and forget it” infrastructure. Important, but largely invisible to most users and internal teams – or something organizations only revisit during certificate renewals, outages, audits, or when new use cases emerge. Certificates are now at the core of service availability, customer confidence, regulatory compliance, and speed to market. If something goes wrong with your certificates, or the processes around them can't keep up, the consequences surface immediately and visibly.

Meanwhile, today's threat landscape is raising the stakes. The most significant breach headlines center on poorly managed cryptographic credentials, such as keys, certificates, and secrets.

Add agentic AI to the picture – with its potential for accessing insecure systems, aggregating information from multiple sources, and accelerating privilege escalation – and the need for strong cryptographic management increases further. Without strong data encryption, strong identity, and robust management of the cryptographic credentials that enable those solutions, AI creates risk at scale that humans can't control.

The operational challenges are also growing. As more business processes go digital, the cost of downtime only increases. Staying on top of industry regulations and government mandates grows harder every year. Failure to apply policy and ensure compliance carries serious consequences.

Put simply, PKI is a business-critical control point for resilience, uptime, and compliance.

The Hidden Business Risks of Certificate Velocity

When certificates expire, the business pays the price.

The biggest risk introduced by 47-day certificates is operational failure at scale – missed renewals, broken integrations, service outages, and audit gaps caused by certificate processes that can't keep up.

Uptime and Availability

Expired certificates take down services, break API integrations, and trigger cascading failures across everything that relies on TLS. The more certificates you have rotating every 47 days, the less time you have to discover a missed renewal before it causes an outage. Mean time to recovery (MTTR) increases when nobody has visibility into or ownership of your certificate inventory.

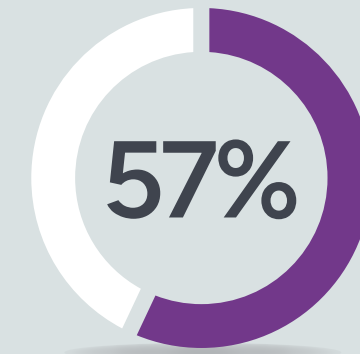
Compliance and Audit Exposure

Managing certificates across disparate sources leads to inconsistent policy enforcement. Disconnected, manual certificate processes leave holes in your audit trail. Between financial institutions, highly-regulated industries, and government entities, failing to demonstrate visibility and control over your certificates could have serious compliance implications.

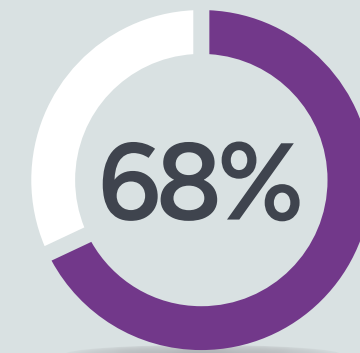
Business and Innovation Impact

When security teams spend their cycles chasing certificate renewals, strategic priorities stall. DevOps pipelines slow and prevent you from executing on your digital transformation strategy. Certificate management overhead compounds with every certificate you manage.

Uptime – Compliance – Business Impact



report that they do not have full visibility into certificates across their organization¹



say managing cryptographic assets is extremely or very difficult¹



experienced outages from certificate failures²

1. 2026 Global State of Post Quantum and Cryptographic Security Trends

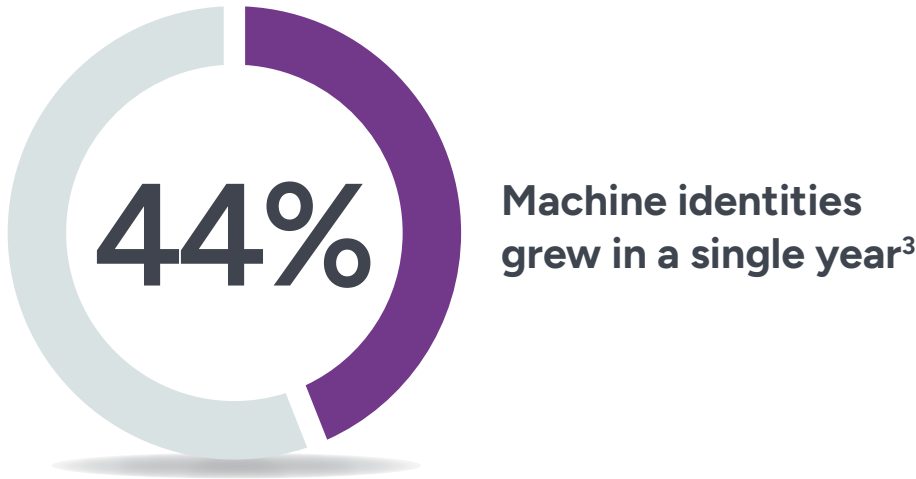
2. Ponemon Institute Trends in PKI Security: A Global Study of Trends, Challenges & Business Impact

Machine Identities Are Multiplying the Challenge

When trust must move at machine speed, manual fails.

As certificate-dependent systems multiply across cloud-native workloads, APIs, containers, IoT devices, and AI-driven environments, the move to shorter public TLS lifecycles becomes harder to absorb. The more systems that depend on certificates, the greater the need for visibility, automation, and control – and 47-day cycles leave no margin for gaps in any of those areas. Even where private trust is more appropriate, organizations still need visibility, ownership, automation, and policy control across a growing machine identity estate.

All these environments create identities that are short-lived, dynamically provisioned, and too numerous to track manually. Trust must happen at machine speed.



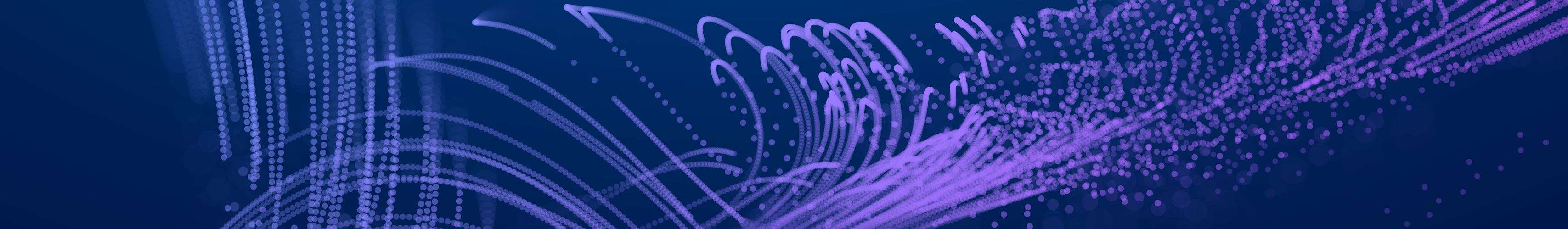
3. RSAC Non-Human Identities (NHIs) Are Growing Faster Than Most Security Programs Blog

PKI is Everywhere

 Web Server	 WFH	 Identity	 CA	 Multi-Cloud
 Cloud	 Network	 File System	 Email	 IoT
 DevOps	 Virtual Machine	 Database	 Mobile	 Applications

The challenge grows under a 47-day model. A certificate securing a containerized workload may need to be issued, deployed, validated, and rotated multiple times before a single manual renewal process is complete. At that frequency, manual processes slow things down and introduce outage risk.

But machine identities don't consist of certificates alone. They also include keys, secrets, and tokens – each with its own management lifecycle, and each a potential attack surface if left unmanaged. Without centralized visibility into every cryptographic asset, an organization can't know what it has, where it lives, or when it expires.



47-Day Certificates as a Foundation for Post-Quantum Readiness

The capabilities you build for 47 days prepare you for what comes next.

New announcements about advances in quantum computing arrive practically every day. Experts estimate that a cryptographically-relevant quantum computer is coming sooner than most organizations are planning for, and Harvest Now, Decrypt Later (HNDL) attacks are already an active advanced persistent threat. In these attacks, adversaries steal sensitive long-life encrypted data today with the intent to decrypt it once quantum computer is capable.

Regulators aren't waiting either. Governments and standards bodies are also accelerating post-quantum planning. NIST has standardized initial post-quantum cryptography algorithms, and guidance from NIST and the NSA calls for widely used RSA and ECC algorithms to be deprecated by 2030 and disallowed by 2035 – increasing pressure on organizations to identify vulnerable cryptography and prepare for large-scale migration.

38% of organizations are actively preparing for the transition to PQC.⁴

The Critical Connection

Knowing the transition to PQC will take several years, organizations need to be preparing now and shouldn't wait before building the necessary capabilities. There's a direct line from mitigating 47-day certificate challenges to post-quantum readiness. That line is crypto-agility.

Crypto-agility is the capability to switch from one cryptographic system to another – whether by changing a configuration setting or enforcing a policy – without impacting the surrounding infrastructure. It rests on three pillars:

- **Visibility** into the certificates, keys, and cryptographic assets that your organization owns, manages, and trusts
- **Policy and control** are necessary to manage the issuance, access, and standards enforcement from a centralized platform
- **Automation** that can deploy and manage those certificates at machine speed

Organizations that build these capabilities to manage 47-day certificates are simultaneously building the foundation for post-quantum migration. Those that don't will face the quantum transition the same way they face the 47-day transition today – reactively, manually, and at significant operational risk.

4. 2024 PKI and Post-Quantum Trends Study

From Certificate Management to Cryptographic Control

Issuing certificates is the easy part, governing them isn't.

The shift to 47-day certificates highlights a distinction that most organizations have never considered. Certificate management is operational. Cryptographic control is strategic.

The difference matters. Organizations focused on certificate management ask: "Do we have all of our certificates up to date?" Strategic organizations ask: "Do we have complete visibility into every cryptographic asset across our environment, and can we enforce consistent policy across all of it?"

That's the question that every organization will be forced to answer once 47-day certificates become the norm.

Under browser-mandated short-validity certificate models, the Certificate Authority (CA) replacement window is moving from roughly one year to 47 days.

What Modern Certificate and Cryptographic Management Must Deliver

To have control over your cryptographic environment at scale, you need a platform that does much more than just issue certificates. Modern PKI must provide capability in these six areas:

1. **Enterprise-Wide Visibility:** Automatically discover and inventory all certificates, keys, secrets, tokens, cryptographic libraries, protocols, and configurations across your organization. If you can't see it, you can't automate it.
2. **Automated Lifecycle Management:** Eliminate manual renewal risk through automated enrollment, deployment, validation, and rollback. Apply that same automation to both public and private PKI.
3. **Policy-Driven Governance:** Define and enforce consistent cryptographic policy across distributed environments. Automatically assess risk, meet audit requirements, and provide on-demand compliance reporting.
4. **Multi-CA Orchestration:** Partner with more than one CA while maintaining the ability to automate certificate issuance and deployment from any, or all, of them. When a CA makes even a minor mistake, browsers can force mass certificate replacement. With short-validity certificates, the window to perform that replacement has compressed from roughly a year to six weeks or less.
5. **Automation-First Operations:** Prepare for the issuance frequency that 47-day certificates require, as well as emergency revocation scenarios like those that can happen on WebPKI in less than one day.
6. **Crypto-Agility by Design:** Design systems with the ability to move between cryptographic standards either by configuration or policy without disrupting the surrounding infrastructure. This capability is a requirement for organizations facing post-quantum migration.

Enabling the Shift With a Platform Approach

Start with scope, then automate everything that follows.

Think platform, not point solutions.

Organizations faced with the coming transition to 47-day certificates will often reach first for tactical fixes, such as automating a subset of certificates here, or adding a monitoring tool there. These approaches address symptoms, not the underlying challenge. Cryptographic risk is an enterprise-wide operational discipline that requires enterprise-wide visibility, control, and automation to manage.

The question isn't whether to automate, but whether your approach can scale to secure what you have today and what you'll need to adopt tomorrow.

Automation is critical to controlling your cryptographic posture. But before you automate, take steps to limit the scope of the problem. For each application, the first question is whether WebPKI is required. If not, then move to private PKI. This eliminates browser policy risk and puts control of the rules back in your organization's court.

For applications that do require public trust, it's worth reassessing which certificate type you're using. Domain Validated (DV) certificates lend themselves to automation far better than Extended Validated (EV) or Organization Validated (OV) certificates, and cost only a fraction of the price. Switching from EV to DV for eligible public trust use cases could cut your public trust spending by up to 99%.

With scope reduced, you can then focus on the type of automation that will account for both routine 47-day rotations and emergency WebPKI revocations, which can trigger in less than 24 hours.

Manual vs. Automated PKI

	Manual PKI	Automated PKI
Certificate Discovery	Incomplete, spreadsheet-driven	Continuous, enterprise-wide inventory
Renewal Process	Calendar reminders, human-triggered	Automated enrollment and deployment
Outage Risk	High – missed renewals equals downtime	Low – no manual gaps in the renewal cycle
Revocation Risk	Hours to days	Minutes – automated replacement triggered immediately
Audit Readiness	Gaps in evidence, manual reporting	Continuous compliance reporting, on-demand
Multi-CA Support	Single CA dependency	Automated issuance across multiple CAs
Scale	Breaks under certificate volume	Designed for machine-speed, high-frequency operations
PQ Readiness	Not designed for crypto-agility	Built to adapt as standards evolve

Prepare Now or Pay Later

What you build now determines how you scale tomorrow.

The move toward 47-day certificates is approaching and organizations that approach it as a certificate management issue will find themselves facing a business resilience crisis. Certificate lifecycles are shortening. Machine identities are multiplying. Post-quantum timelines are accelerating. Each of these is significant on its own, but together, they paint a clear picture. There's a narrow window to lay the groundwork for a resilient cryptographic infrastructure, and it's open right now.

The consequences of inaction are real – service outages that disrupt your brand and business, compliance violations that result in fines, and operations that simply break down under the volume that shorter-lived certificates require.

But the opportunity is also real. Organizations that modernize now lower operational risk, ensure business resilience, and lay the cryptographic foundation needed for the post-quantum future. The visibility, automation, policy control, and crypto-agility you build to solve for 47-day certificates will be what differentiates success from chaos when it's time to migrate to post-quantum algorithms.

See how the [Entrust Cryptographic Security Platform](#) helps organizations reduce certificate risk, automate lifecycle management, and build the crypto-agility needed for what comes next.

Your Action Plan



1. Assess your PKI Strategy:

Are you using the right PKI for your use cases? Wherever possible, consider private PKI. By removing the browser from the equation, you eliminate policy risk and regain control.



2. Establish Discovery and Visibility:

Inventory certificates, keys, and cryptographic assets across users, machines, applications, and environments. Understand how they're exposed to risks like short-lived certificate validity, revocation events, and manual renewal processes.



3. Automate:

Automate enrollment, deployment, renewal, and rollback to survive shortened certificate lifetimes. Test automation through failure scenarios and apply it to your private PKI deployments too.



4. Build Resilience:

Diversify your reliance on any single Certificate Authority. Plan for issuer, policy, and operational failure modes – especially if you work with WebPKI.



5. Centralize Control:

Define cryptographic program ownership. Establish clear roles and decision-making authority and implement technology to enforce policy, identify risks, and remediate where necessary.



6. Use 47-Day Certificates as a Proving Ground:

Build the systems and processes you'll need to continue adapting to an ever-changing crypto landscape. Once you do, your organization will be ready to operate, scale, and innovate securely – today, tomorrow, and post-quantum.

ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit entrust.com.

entrust.com | Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

©2026 Entrust Corporation. All rights reserved. Entrust and the hexagon logo are trademarks, registered trademarks, and/or service marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners.
DS27Q1-47-day-certificates-pki-eb



ENTRUST

SECURING A WORLD IN MOTION