BUYER'S GUIDE

The Foundation of Digital Trust: A Buyer's Guide to PKI

ENTRUST

SECURING A WORLD IN MOTION

INTRODUCTION

PKI at a Turning Point

Public key infrastructure (PKI) has long been the foundation of digital trust – quietly securing people, devices, applications, and data across every environment. But the landscape it supports is shifting fast.

Organizations now rely on an expanding ecosystem of digital identities, from cloud workloads to the Internet of Things (IoT), with the average enterprise managing more than 55,000 certificates.[1] As environments grow more distributed, the systems that maintain trust must evolve alongside them.

At the same time, certificate lifetimes are shortening, regulations are becoming more stringent, and post-quantum cryptography (PQC) is on the horizon. These forces introduce new urgency into what was once a stable, predictable discipline. Today, security and compliance teams must maintain uptime, reduce operational risk, and support continuous audit readiness – all while facing greater complexity than ever before.

Use our guide to explore the challenges reshaping PKI, the options available to buyers, and how to modernize trust for the future.

The Challenge: Complexity, Compliance, and Change

As organizations modernize their environments, the trust landscape around them is becoming far more dynamic – and significantly harder to manage. PKI underpins cloud, identity, and regulatory frameworks, but several accelerating forces are reshaping how enterprises must maintain it:

- **Shorter certificate lifetimes:** Publicly trusted certificates have a current validity period of 398 days, but a recent ballot passed by the CA/B Forum mandates that the lifetime will be reduced to 47 days by 2029, increasing the operational complexity and risk.[2] It's no surprise 94% of security leaders worry about their ability to manage these shorter lifespans as renewal cycles intensify.[3]
- **Post-quantum threat:** Cryptography itself is evolving. Current public key algorithms in use today will no longer be secure once acryptographically relevant quantum computer (CRQC) is realized. The transition to quantum-safe algorithms will require organizations to touch every single cryptographic system and infrastructure.
- **Operational complexity:** Most enterprises now manage years of accumulated cryptographic systems, tools, and legacy technologies. This "cryptographic sprawl" leads to fragmented visibility and inconsistent policies and processes, all while needing to oversee the lifecycle of thousands of keys, certificates, and secrets that must be tracked, automated, and governed to reduce risk and technical debt.
- **Compliance pressure:** Many regulatory frameworks require demonstrable control over cryptographic assets. That's a growing challenge when 83% of organizations already experience at least one certificate-related outage each year.[3]

Combined, these forces are reshaping how enterprises must think about PKI – not as a static tool, but as a living system that needs to evolve.

47 days

By 2029, TLS/SSL TLS/SSL certificates will be valid for only 47 days, meaning organizations need to prepare to manage renewals.

83%

of organizations already experience at least one certificate-related outage each year.

Why PKI Still Matters

Even as digital environments evolve, PKI remains one of the most reliable methods for establishing and maintaining trust. At its core, PKI provides identity, encryption, and integrity – the foundational capabilities that allow people, systems, devices, and applications to remain secure. Every authenticated login, encrypted session, signed document, and trusted machine-to-machine exchange depends on these principles working consistently behind the scenes.

PKI also plays a central role in Zero Trust strategies, cloud security architectures, and modern compliance frameworks. As organizations adopt new technologies and shift more workloads to hybrid and multi-cloud environments, the ability to verify identities and protect data at every touchpoint becomes even more critical.

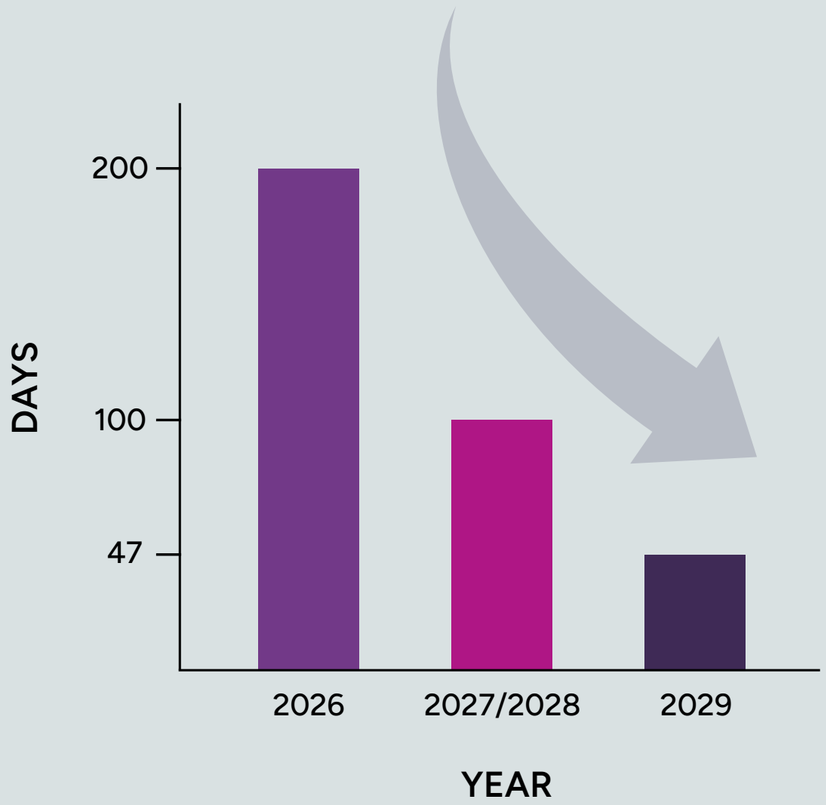
PKI has always required deep expertise – from defining certificate policies to operating secure, audited infrastructure. As environments expand and lifecycles accelerate, maintaining PKI becomes even more challenging. The issue isn't with PKI's value, but with managing that complexity across hybrid systems and evolving regulations. With the right design and governance in place, PKI remains a strong, reliable foundation for digital trust.

Public Trust: Essential but Increases Risk and Operational Complexity

Publicly trusted PKI – commonly known as WebPKI – provides the foundation for secure communication across the open internet. Browsers, operating systems, and applications depend on it to authenticate public-facing websites and encrypt data in transit. For these external use cases, public trust will always remain the only viable and correct model.

The challenge arises because public trust is governed by the CA/Browser Forum, which limits how organizations can use and control these certificates. Several internal use cases – including internal applications and web servers, code signing for internal systems, and POS terminals – are common examples where public trust is often used but not required. As certificate lifetimes shorten to 200 days (2026), 100 days (2027), and 47 days (2029), renewal cycles increase exponentially. This creates significant operational risk, renewal churn, and outage potential that manual processes simply cannot absorb. It is also ideal to evaluate these eligible use cases and move them to private trust where possible.

Lack of visibility further complicates matters: 74% of organizations don't know how many certificates they have, making it far easier for public certificate to sprawl into private environments without proper oversight.[4] Even when used appropriately, frequent renewals and revocations make lifecycle automation essential. Pairing public certificates with automated discovery and renewal ensures public trust remains reliable without introducing avoidable complexity.



Private PKI: Taking Control of Trust

For many organizations, private PKI offers the control and flexibility needed to secure internal applications, devices, and digital identities. It enables enterprises to define policies, naming conventions, and validity periods that reflect their environment – not the requirements of public trust ecosystems. This makes private PKI well-suited for use cases such as:

- Internal servers and applications
- Mobile Device Management
- Virtual Private Network access
- DevOps workflows
- IoT deployments

Private PKI also helps reduce reliance on public certificates for eligible use cases, allowing organizations to tailor certificate lifecycles and issuance processes to their specific needs. However, this control comes with responsibility. Running an internal PKI requires specialized skills, secure hardware, continuous monitoring, and regular audits to ensure governance alignment and regulatory compliance.

As certificate volumes grow and environments become more complex and distributed, many organizations are now evaluating their overall PKI strategy and whether they should adopt managed or platform-based PKI models. These approaches offer the same level of control, but without the resource burden of maintaining PKI infrastructure and operations in-house.

PKI and Compliance: Meeting Evolving Standards

As security and privacy regulations become more prescriptive, PKI plays an increasingly important role in demonstrating compliance, particularly with frameworks like the:

- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Digital Operational Resilience Act (DORA)
- Network and Information Systems Directive (NIS2)

PCI DSS, HIPAA, DORA, and NIS2 all require organizations to show clear control over cryptographic operations – including how keys and certificates are issued, stored, rotated, and retired. PKI provides the mechanisms to enforce identity verification, protect sensitive data, and maintain integrity across systems and transactions.

However, the compliance landscape is not static. The transition to quantum-safe cryptography will require organizations to replace and reconfigure large portions of their cryptographic systems and infrastructure, adding new complexity to audit preparation and ongoing governance. Manual processes simply cannot keep pace, and current systems need to be evaluated.

Automated PKI operations and certificate lifecycle management (CLM) tools help organizations maintain accurate inventories, enforce policy consistently, and produce verifiable audit trails. With greater visibility and automation in place, teams can adapt to regulatory change without sacrificing operational efficiency or security.

Managed PKI: Expertise Without the Overhead

As PKI environments become increasingly complex, and there is a shortage of internal skills and expertise, many organizations are turning to managed PKI or cloud-hosted PKI as a Service (PKIaaS) options to reduce operational burdens while maintaining strong security and policy control. In these models, CA and registration authority (RA) functions are operated by cryptographic experts who follow rigorous, audited best practices.

Managed PKI is especially valuable for regulated industries such as finance, healthcare, and government, where audit requirements demand verifiable assurance and continuous compliance. It provides predictable scalability, highly resilient operations, and integrated CLM, helping teams prevent outages and simplify governance across distributed systems.

By leveraging a managed service, organizations can eliminate the operational complexity of running PKI in-house while ensuring their certificate infrastructure remains secure, up to date, and aligned with evolving regulatory and cryptographic requirements.

PKIaaS at a Glance:

Organizations retain full oversight of policies, use cases, and certificate profiles – without the need to maintain hardware, staffing, or 24/7 monitoring.

The Next Evolution: PKI in the Cryptographic Security Platform

Many organizations are recognizing that traditional PKI – even when modernized – is only one part of a much larger trust ecosystem. The Entrust Cryptographic Security Platform (CSP) brings these components together, unifying PKI, hardware security modules (HSMs), keys/certificates/secrets management, and compliance management – all under a single governance model.

CSP includes a comprehensive, high-performance, container-based PKI, CLM, and automation solution. It comprises all the components required to run a secure, quantum-ready PKI, deploy in a range of applications, and expand on demand. It enables customers to streamline PKI and CLM while providing the flexibility to scale across enterprise and cloud environments.

The platform also provides centralized dashboards, automated workflows, and post-quantum readiness, helping organizations prepare for the cryptographic transition without disrupting business operations. This unified approach simplifies lifecycle management, enhances compliance, and prepares organizations for the post-quantum era.

Cryptographic Security Platform

- Gain unparalleled security and visibility
- Achieve operational efficiency
- Automate monitoring and compliance management
- Built-in crypto-agility and post-quantum readiness

The Entrust Advantage: Pioneers in PKI

Entrust has helped organizations establish and maintain digital trust for more than 30 years. As the provider of the world's first commercially available PKI in 1994 – and the first PQ-ready PKI in 2024 – Entrust continues to lead the industry in cryptographic innovation, assurance, and expertise.

Strong PKI depends on strong key protection, which is why HSMs are used to generate and safeguard the private keys at the heart of every certificate authority. As a result, HSMs are one of the primary building blocks for secure, compliant PKI deployments.

Today, Entrust offers one of the most comprehensive PKI portfolios available. Enterprises can deploy PKI on-premises, leverage managed PKI for expert-led operations, or adopt CSP to unify cryptographic management across their environment. All Entrust PKI offerings are architected according to best practices, underpinned by nShield HSMs, and backed by deep experience supporting security-critical sectors around the world.

Beyond technology, Entrust's professional services teams help organizations design, deploy, modernize, and migrate their PKI environments with confidence. Whether it be addressing compliance requirements, scaling across hybrid environments, or preparing for quantum-safe transitions, Entrust provides the trusted foundation for long-term resilience.

Build Lasting Trust for What's Next

Cryptography is entering a period of rapid transformation. Certificate lifetimes are shrinking, new regulations are emerging, and the transition to quantum-safe algorithms will require organizations to rethink how they manage trust. PKI remains central to this process – but it must be modernized to keep pace with evolving risks and operational demands.

Entrust helps organizations manage and automate every aspect of PKI through trusted, PQ-ready solutions built for the next generation of cryptography. The future of trust starts with visibility, automation, and assurance – all delivered through Entrust's decades of leadership and innovation.

By establishing a modern, resilient PKI foundation today, organizations can reduce operational risk, simplify compliance, and position themselves for the post-quantum world. The path to lasting trust begins with clarity, control, and a partner proven to lead the way.

Ready for what's next?

Explore how Entrust PKI and the Cryptographic Security Platform can help your business prepare for the future.

Sources

1. https://securityboulevard.com/2024/10/digicert-its-a-matter-of-trust/

2. https://www.businesswire.com/news/home/20250414207334/en/CABrowser-Forum-Passes-Ballot-to-Reduce-SSLTLS-Certificates-to-47-Day-Maximum-Term

3. https://www.cyberark.com/resources/white-papers/organizations-largely-unprepared-to-manage-47-day-tls-certificates

4. https://www.certisur.com/en/news/the-time-to-automate-your-digital-certificate-management-has-arrived/

ABOUT ENTRUST CORPORATION

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

ENTRUST
SECURING A WORLD IN MOTION