PKI Meets PAM: Navigating Shrinking Certificate Lifespans

A practical guide for identity security and architecture teams on aligning PKI and PAM to manage accelerating certificate lifecycle demands.

INTRODUCTION

Why PKI and PAM Must Converge as Certificate Lifespans Shrink

For years, trust was established through centralized Certificate Authorities (CAs) issuing certificates with long lifecycles, making Public Key Infrastructure (PKI) a largely administrative function revisited infrequently. **Shrinking TLS certificate lifespans have fundamentally changed this model. What was once a periodic task is now a continuous operational requirement with direct implications for availability and resilience.**

At the same time, the long-standing separation between Privileged Access Management (PAM) and PKI is creating operational blind spots. When these controls operate independently, gaps emerge around ownership, automation, and change control that undermine reliability at scale.

Machine identities now outnumber human identities by orders of magnitude. To maintain trust in modern, distributed environments, organizations must align human and machine identity controls. **Converging PAM and PKI enables consistent governance, reduces operational risk, and ensures identity-driven architectures can meet today's security and availability demands**.

Table of Contents

PART ONE

Strategic Roles of PKI and PAM

PAM protects and monitors privileged access by enforcing controls around elevated activity. It answers the question of **who is accessing critical systems**.

PKI establishes cryptographic trust across infrastructure by authenticating servers, devices, workloads, and services. It answers the question of **what is trusted**.

As machine identities scale, **PKI can no longer operate as a standalone function**. Certificate based trust must align with privileged access controls, governance models, and Zero Trust execution.

When PKI and PAM operate together, organizations gain real-time visibility into every trust relationship, from employees to automated workloads. Coupled with governance tools, organizations unlock unified visibility across all identities, coordinated automation that links certificate trust events to their privileged access counterparts, and consistent audit narratives aligned to Zero Standing Privileges and cryptographic agility.

The result is a cohesive identity fabric where trust is enforced consistently across people, systems, and workloads.

Keep reading: The next page outlines the strategic roles of PKI and PAM in modern identity architecture

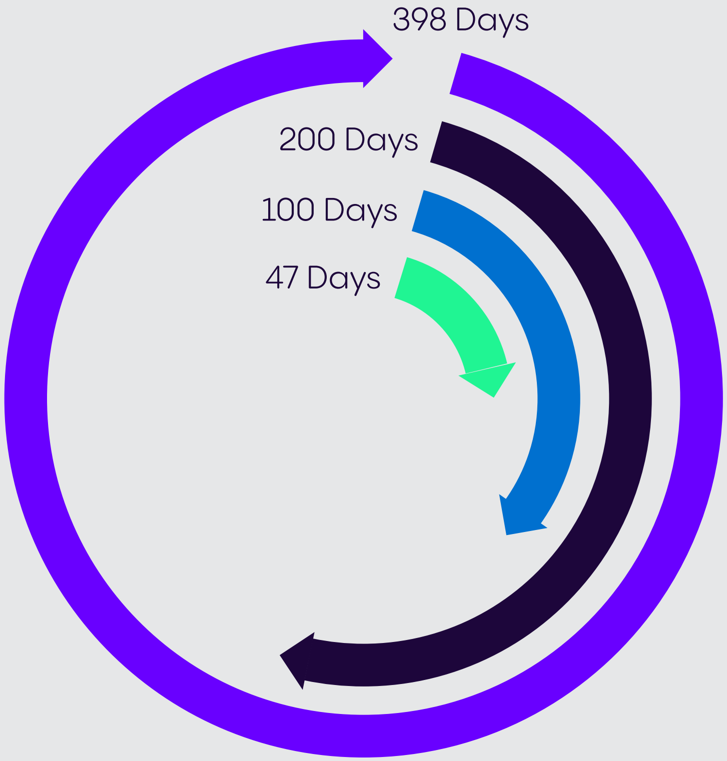
PKI and PAM Roles in Modern Identity Architecture

	PAM (Who)	PKI (What)
Primary Purpose	Control, monitor, and govern privileged access to systems	Establish cryptographic trust between machines, services, and infrastructure
Identity Scope	Human and service users, interactive workflows, system services	Machines, websites, IoT devices and network infrastructure, web applications
Authentication Subject	Users, services or applications operating as a privileged identity	Certificates and their private keys assigned to machines and workflows
Key Controls	Just in time (JIT) access, Zero Standing Privilege, least privilege, MFA, session recording, policy enforcement	Certificate issuance, renewal, rotation, revocation, and CA policy enforcement (EKUs, SANs)
Ideal Lifecycle	Request → Approve → Provision at least privilege → Monitor → Elevate if necessary → Decommission	Discover and Inventory → Issue → Deploy → Renew or Rotate → Revoke Certificate
Automation Scope	Accounts discovery, conditional access and approval workflows, credential rotation and validation, session controls	Discovery, enrollment (ACME/SCEP), automated renewal/rotation, compliance validation
Operational Metrics	Password compliance metrics, integration with JML lifecycle, PSM adoption and facilitated session usage, successful DR liveplay and breakglass readiness validation, audit pass rates	Automated renewal success rates, inventory coverage percentage, outage safety net, policy conformity

PART TWO

The Certificate Renewal Challenge

TLS certificate lifespans are shrinking, from 398 to 200, 100, and soon 47 days, creating an exponential surge in renewal volumes by 2029.



New guidance from the Certification Authority (CA)/Browser Forum is dramatically **shortening certificate validity periods from 398 days to just 47 days by 2029**; a reduction of 88% of the current lifespan. This shift fundamentally alters the operational burden of certificate management.

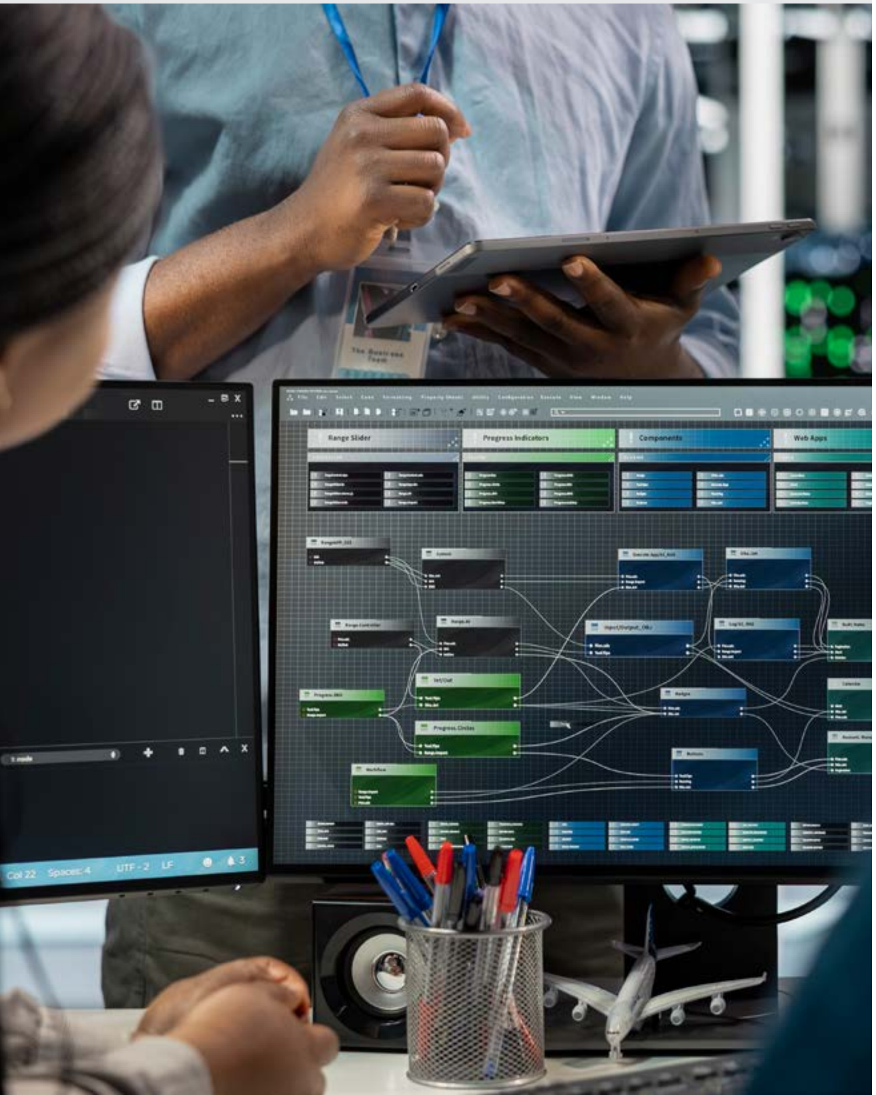
The impact has immediate implications:

- **Renewal volume increases exponentially** as certificates must be replaced multiple times per year
- **The risk of critical systems encountering a communication-based outage increases** when a single missed renewal cascades across unknowingly dependent systems
- **Distributed and cloud-native environments introduce blind spots** as containers, ephemeral workloads, and multi-cloud platforms generate more machine identities than traditional PKI tooling can track
- **Compliance exposure rises** as certificate failures surface during audits
- **Hidden operational fragility emerges** when renewal tasks become single points of failure

Certificate operations can no longer be treated as a background task. They are now a core resilience control that must be addressed through automation, unified governance, and architectural strategies.

PART THREE

Automation as a Critical Enabler



Manual certificate management cannot scale as lifecycles shrink. **Automation is the only viable path to sustaining trust at enterprise scale**.

However, **simple scripting is insufficient**. Scalability places heavy demands on automation reliability, exception handling, and operational maturity. **Organizations require a flexible, policy-driven framework** rather than one-off tooling.

An effective automation framework should:

- Provide a flexible centralized foundation across all aspects of your environment and visibility into your PAM and PKI intersections
- Normalize automated certificate issuance, renewal, rotation, and revocation by increasing efficiency and removing human error
- Clearly track control effectiveness with measurable operational metrics
- Maintain a unified certificate ledger to enforce cryptographic policy and agility

A practical test of maturity is simple:

> **Can your organization rotate cryptographic standards across your environment within a single certificate lifecycle?**

If not, automation gaps are likely to increase risk rather than reduce it.

PART THREE

Five Steps to Mature Machine Identity Management

Modern machine identity programs require a staged, architectural approach. These steps provide a clear path to maturity while unifying PKI, PAM, and governance into a single operating model.

1. **Elevate Urgency**
   Position shrinking certificate lifespans as a resilience and business risk to secure executive support.

2. **Automate Discovery and Renewal**
   Identify critical certificates and eliminate renewal gaps through automated lifecycle controls.

3. **Integrate Compliance**
   Embed audit-ready controls aligned with regulatory and Zero Trust requirements.

4. **Unify Identity Governance**
   Align privileged access and machine identities undercentralized, policy driven oversight

5. **Extend Automation Scope**
   Expand protection to secrets, API credentials, and emerging non-human identities

This phased approach delivers immediate operational value while establishing long-term architectural resilience.

CONCLUSION

Next Steps Toward Unified Machine Identity Governance

Machine identity management is now a core component of enterprise security architecture. Certificate failures trigger outages, broken integrations, and compliance violations with significant business and reputational impact.

Identity security and architecture teams must modernize how PKI, PAM, and automation frameworks operate together under a unified governance model. Aligning human and machine identity controls ensures trust remains scalable, resilient, and auditable as certificate lifecycles continue to compress.

Take the Next Step

If your organization is ready to advance **unified machine identity governance** and **align PKI and PAM at scale, MajorKey can help.**

Working alongside **CyberArk**, we help identity teams assess maturity, design integrated automation strategies, and implement resilient, audit-ready controls that scale with the business.

Scan the QR code or click here to contact us and learn more.

Visit our CyberArk resource hub to explore additional resources and best practices.

MajorKey CYBERARK