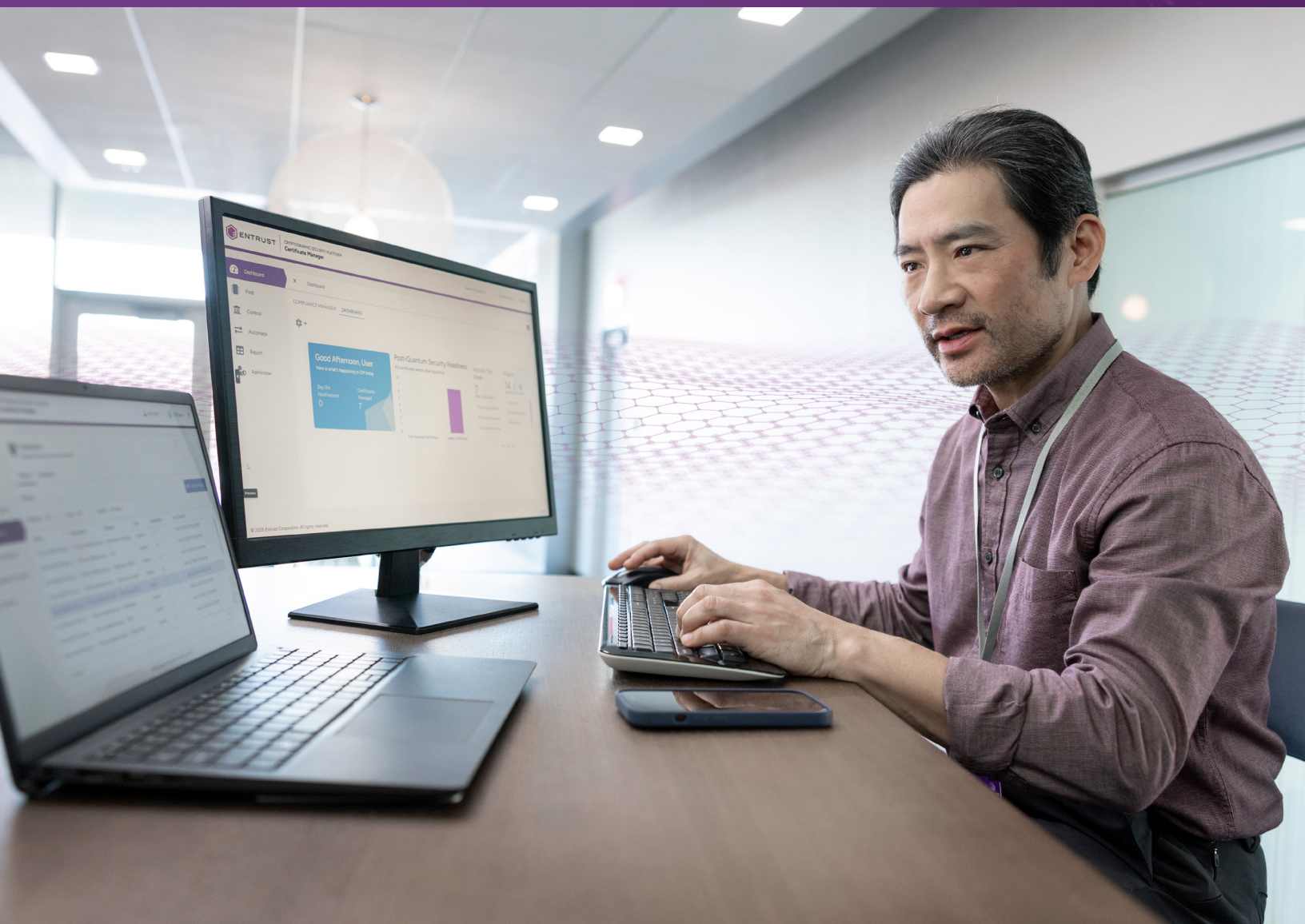


# Key and Certificate Lifecycle Management

## Take Control of Your Cryptography



**ENTRUST**  
SECURING A WORLD IN MOTION

## The Challenge: Managing Keys, Certificates & Secrets at Scale

Modern IT environments generate an explosion of cryptographic assets – including keys, certificates, and secrets – across cloud, on-premises, and hybrid infrastructure. Left unmanaged, these assets become operational blind spots that could lead to outages, security risks, compliance failures, and expanding attack surfaces.

These challenges are intensifying as organizations face dramatically shorter certificate lifetimes, fragmented ownership across teams and tools, rapid growth in machine identities, and the urgent need to build cryptographic foundations for a post-quantum future – often all at the same time.

## The Pressure is Real: Why Lifecycle Management is Now a Business Risk

### 47-Day Certificates Turn Manual Processes into Operational Risk

The shift to 47-day certificate lifetimes fundamentally changes the economics of certificate management. What was once a periodic task is now a continuous operational burden. Manual tracking, renewal, and deployment processes simply cannot scale – leading to expired certificates, unplanned outages, and emergency remediation that disrupts both security and business operations. Without automation and centralized lifecycle management, organizations are forced into a constant reactive posture.

### Lifecycle Sprawl: Too Many Assets, Too Many Owners, Too Little Visibility

Keys, certificates, and secrets now exist everywhere – across applications, containers, APIs, devices, workloads, and identities. Ownership is often fragmented across security, DevOps, platform, and application teams, each

using different tools and processes. The result is lifecycle sprawl: unmanaged cryptographic assets, inconsistent policies, and limited visibility into where sensitive material exists, how it's protected, or when it expires. This sprawl increases attack surfaces, audit complexity, and operational risk.

### Post-Quantum Readiness Raises the Stakes for Crypto-Agility

At the same time, organizations must prepare for the transition to post-quantum cryptography. This isn't an algorithm swap but instead requires visibility into where classical cryptography is used, control over lifecycle processes, and the ability to rotate, reissue, and migrate cryptographic assets at scale. Without strong lifecycle management foundations, post-quantum migration becomes slow, risky, and operationally disruptive.

## The Opportunity: Centralized Lifecycle Management with PQ Preparedness

Organizations that unify lifecycle management for keys, certificates, and secrets gain the ability to:

- Achieve full inventory and visibility of cryptographic assets – eliminating unmanaged keys, secrets, and certificates
- Streamline issuance, rotation, renewal, revocation, and retirement across environments and tooling
- Enforce enterprise-wide policy, audit and compliance mandates (including 47-day readiness timelines)
- Strengthen crypto-agility – enabling controlled transitions between cryptographic algorithms and future post-quantum standards

This approach reduces risk, minimizes manual effort, and prepares security teams for both current operational demands and future PQC migrations.



PQC readiness timelines have accelerated with NIST planning to deprecate RSA and ECC by 2030 and fully disallowing by 2035.

# Entrust Cryptographic Security Platform – A Unified Solution

The Entrust Cryptographic Security Platform (CSP) provides a unified lifecycle management solution for keys, certificates, and secrets – bringing them together with policy-driven automation, centralized visibility, and crypto-agility across the enterprise.

## Key Capabilities:

### PKI & Certificate Lifecycle Management (CLM)

- Container-based PKI and robust CLM for discovery, automated renewal, certificate orchestration, and revocation

### Key & Secrets Lifecycle Management

- Automated key and secret creation, storage, rotation, and retirement – secured and auditable across teams and systems

### Centralized Visibility & Policy Enforcement

- A single dashboard showing all cryptographic assets, with policy-based controls to enforce compliance, governance, and risk standards

### 47-Day Certificate Compliance

- Automatic certificate tracking and renewal workflows eliminate manual intervention and help mitigate the risk of expired credentials

### PQC-Ready & Crypto-Agile

- Built-in support for crypto-agility and integration with PQ-ready components ensures you're prepared for evolving standards, including post-quantum algorithm adoption

## Take Control of Cryptographic Lifecycles – Today, and for What Comes Next

Shorter lifecycle lifetimes, expanding machine identities, and post-quantum timelines are converging into a single reality: cryptographic lifecycle management can no longer be fragmented, manual, or reactive. Organizations that centralize visibility, automate lifecycles, and build crypto-agility now will be best positioned to reduce outages, strengthen security, and transition confidently to post-quantum cryptography.

Entrust helps organizations turn cryptographic complexity into control – creating a resilient foundation for today's operations and tomorrow's cryptographic challenges.

### Talk to an Entrust Expert

Timelines are moving fast. Learn how Entrust can simplify certificate lifecycle management and help you prepare for the post-quantum transition. [Connect with an Entrust expert today.](#)

## Solution Benefits:

### Avoid Unplanned Outages

- Automated lifecycle processes prevent sudden certificate expiration and service disruptions

### Improve Security & Reduce Attack Surfaces

- Visibility and automation reduce unmanaged keys and secrets before adversaries can exploit them

### Support Regulatory & Industry Mandates

- Policy enforcement and audit trails simplify compliance with both internal standards and external regulatory controls

### Future-Proof Cryptographic Infrastructure

- Crypto-agility capabilities and PQ-roadmap support ease the transition to post-quantum cryptography

Organizations face an 8x increase in operational overhead and risk by 2029 when 47-day certificates are mandated.

## 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 [www.entrust.com](https://www.entrust.com).