# Removing the Complexity and Guesswork from Your PKI Refresh

## Successfully transition with automated security and validation

## The Facts

**45% of Companies**
Admit that failing PKI management results in lost trust[1]

**17,800+ Keys and Certificates**
Are in today's average enterprise[1]

**200+ Certificates**
Become unwieldy to track, according to Gartner[2]

**51% of Organizations**
Are unaware of how many keys and certificates are in use[1]

**2 Certificate-related Outages**
Have occurred on average in each Global 2000 organization over the last two years[3]

**$14.6M is the Cost**
Of an average certificate-related outage in the Global 2000[3]

## PKI Refresh Challenges

Public key infrastructure (PKI) is the foundation of today's enterprise security. From SSL/TLS authentication of web services to new industry-specific devices and networks of things, businesses and governments are using more digital certificates from more trusted third parties and internal sources. The replacement of expiring internal Certificate Authorities (CAs), new security and compliance requirements, and an evolving threatscape are increasing the difficulty and cost of revamping PKI.

As new root or intermediate CAs are generated, establishing these CAs in hundreds or thousands of distributed applications' certificate trust stores proves a daunting, expensive, and often error-prone project. Differing, distributed applications as well as administrators unfamiliar with certificates or trust stores prove especially difficult. Most PKI lacks central visibility, consistent processes, and refresh progress validation. This leads to errors and missed system updates that result in policy violations and costly business interruptions.

## Impact on Your Security

Over the last two years, more than 2300 global businesses experienced a security incident involving misused or compromised certificates.[1] "PKI is under attack," simply stated Scott Charney, VP Trustworthy Computing at Microsoft, during his keynote speech at the RSA 2013 conference. In response to these threats, organizations are adopting these PKI updates:

- **Shorter certificate lifetimes:** Google and others are shortening certificate lifetimes to 3 months or less, reducing certificate risk exposure.
- **New security standards:** NIST and CAs are replacing SHA-1 with SHA-2. Experts believe SHA-1 attacks are now feasible[4] and browsers will identify SHA-1 certificates as less trusted in 2015.
- **New compliance rules:** Regulations (e.g., PCI DSS) and security frameworks (e.g., SANS 20 Critical Security Controls) have updated rules on maintaining digital certificates.
- **New remediation strategies:** Research from Netcraft, University of Maryland, and Venafi show that most organizations did not completely replace certificates vulnerable to Heartbleed, remaining exposed.

VENAFI

To learn more visit
Venafi.com/PKIRefresh

Venafi automates, streamlines, and validates your PKI refresh, scaling to hundreds of thousands of keys and certificates. And with automated integration across hundreds of applications, devices and CAs, you can deliver policy-enforced replacement or remediation of certificates in just minutes.

Most administrators have no way to manage and validate their PKI refresh progress—blind to where they are in the transition or if it is complete.

## Successful PKI Refresh

With today's fast changing threatscape and increasing use of digital certificates, successful PKI refreshes require complete visibility, enforced policies and workflows, and automation.

### Complete Visibility

- Discovery of all certificates and trust stores
- On-going monitoring and progress tracking

### Enforced Policies and Workflow

- Flexible criteria such as certificate lifetime, authorized CA, and more
- Certificate ownership assigned to individuals or groups
- CA and certificate installation and configuration using established policies and workflows

### Automated PKI Refresh

- Streamlined and validated PKI refresh with reports on progress and completion
- Installation and whitelisting of new root or intermediate CAs across applications
- Policy-enforced, self-service portal for certificate issuance and renewal
- Automated certificate renewals or replacements with installation validation

## Venafi Trust Protection Platform

Venafi Trust Protection Platform, with Venafi TrustAuthority™ and Venafi TrustForce™, enable you to automate your PKI refresh.

## Venafi TrustAuthority

### Enables Visibility

- Identifies all keys, certificates, CAs, and trust stores across enterprise networks, the cloud, and multiple CAs
- Uses a baseline to identify misuse

### Enforces Policies and Workflows

- Provides a policy-enforced, web-based, self-service portal for certificate requests and renewals
- Enforces configurable workflows capabilities for replacement, issuance, and renewal
- Tracks progress and completion of PKI refresh with real-time dashboards and detailed reporting

## Venafi TrustForce

### Automates Management and Security

- Automates and validates the entire CA and certificate refresh process
- Distributes and whitelists new CAs in trust stores
- Replaces certificates in seconds, integrating with dozens of internal and external CAs
- Remediates across thousands of certificates in just hours in the event of a CA compromise or new vulnerability such as Heartbleed

## PKI Secures Trust

Your PKI holds the keys and certificates that are the foundation of trust for all of your critical systems and your interactions with customers and partners. You can secure this trust with Venafi, achieving an automated PKI refresh that eliminates outages caused by expired certificates, roots, and intermediates and accelerates the upgrade to the more secure SHA-2 algorithm, while also improving your security posture and reducing risk.

## About Venafi

Venafi is the leading cybersecurity company in Next Generation Trust Protection. Venafi delivered the first trust protection platform to manage, secure, and protect cryptographic keys and digital certificates that every business and government depends on for secure communications, commerce, computing, and mobility.


1. Ponemon Institute. *2013 Annual Cost of Failed Trust Report: Threats & Attacks*. 2013.
2. Ouellet, Eric and Wheatman, Vic. Gartner. *X.509 Certificate Management: Avoiding Downtime and Brand Damage*, November 4, 2011. Gartner Document: G00226426.
3. Ponemon Institute. Unpublished Survey Results for the *2013 Annual Cost of Failed Trust Report: Threats & Attacks*. 2013.
4. Cobb, Michael. TechTarget. *SHA-2 Algorithm: The How and Why of the Transition*, October 2014.





Part number: 1-0031-0115


VENAFI

To learn more visit
Venafi.com/PKIRefresh