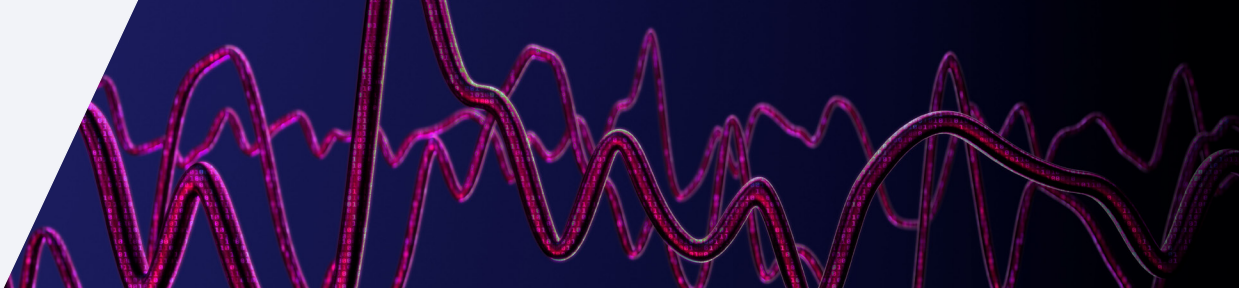
Venafi



DATA SHEET

Private PKI, Fast and Easy

Venafi Zero Touch PKI Secures Your Distributed Teams, Networks and Devices

Zero Touch PKI at a Glance

Venafi Zero Touch PKI is an SaaS-based alternative to the cost and hassle of creating, issuing and maintaining privately trusted X.509 digital certificates for your network systems, devices and users.

- Delivers ready-made digital certificate issuing profiles for mobile and network devices
- Deploys flexible root and intermediate issuing CA hierarchies to fit business needs
- Autoenrollment and automated issuance for Microsoft desktops and laptops
- Rotate, replace or revoke any group of certificates in real time

Maintaining your own private PKI is expensive and hard. Refreshing or migrating to a new PKI requires expertise and knowledge you may not have.

Benefits

- Simplify your private PKI through a fully managed, SaaS-based service
- Replace brittle, outdated systems with modern, fast PKI architecture
- Focus scarce resources on high-benefit projects while Venafi maintains your internal PKI

Recent changes in technology and society have stressed the first-generation PKI (public key infrastructure) systems that maintain and distribute internal TLS certificates to their breaking points. Network admins, developers and knowledge workers have all become remote employees, each needing stronger machine-to-machine authentication and encryption on the systems they rely on. Established PKIs are expiring when security teams are overburdened with more work than ever before. At the same time, organizations are increasing the speed and urgency of their digital transformation efforts.

Many PKI teams are already working with brittle, hard-to-maintain internal PKI systems that require constant care and immediate updates. Now, seemingly overnight, the number of sites and services needed to serve customers and partners has doubled or tripled, requiring even more attention from already strapped teams. In many cases, this has created a painful three-way collision: Internal teams have less time, but they are also responding to exponentially more requests that carry an even higher level of urgency.

Venafi is the inventor and creator of the machine identity management category. With 20 years of innovation in PKI, Venafi is the trusted partner who can deliver a turnkey, state-of-the-art internal PKI service that is cost-effective, sets up fast and delivers time-to-value even faster. It also meets the scalability and residency needs of businesses with global data center operations.

Challenges

PKI has always been hard. It's a complex system that demands a level of expertise that is difficult to find and retain, especially as the number of machine identities that organizations need to remain secure skyrockets. But recently, a number of emerging challenges have transformed what has been a difficult task to an almost impossible one.

Updating Windows PKI. Many organizations have built their private PKI on Microsoft Active Directory Certificate Service (ADCS), the Windows server role that allows them to provide public key cryptography, digital certificates, and digital signature capabilities to their organization. Now they find themselves unable to keep up with the steady stream of patches, updates, hot fixes and vulnerabilities Microsoft requires with AD and SQL Server. These Microsoft PKIs are expiring and must be refreshed on unforgiving deadlines.

Modernizing PKI. Many internal PKI systems were built on older processes and standards, but PKI requirements in these standards are evolving rapidly. As recently as September 2020, the multinational Internet Engineering Task Force (IETF) updated RFC-8894, the specification standard for Simple Certificate Enrolment Protocol (SCEP). For most organizations, keeping up with these new recommendations and best practices is arduous and time-consuming. Unfortunately, cybercriminals are increasingly targeting machine identities—so updates are no longer optional.

Demonstrating Security, Proving Compliance. The list of regulatory standards, security frameworks and compliance mandates that verify the robustness and integrity of internal encryption processes continues to grow. PCI DSS, NIST and ISO have all added requirements for stronger cryptography and updated protocols in recent releases. In addition, industry-specific mandates, like NERC CIP requirements for energy providers and FFIEC for banking, are likely to respond to the increase in remote working with new machine-to-machine requirements in the near future.

Moving PKI to the Cloud. Cloud platforms offer a similar set of benefits across many different technology areas: the ability to scale up and down rapidly as business demands change; manageable and forecastable costs; and the flexibility needed to rapidly support new initiatives. PKI is no exception. Cloud-based PKI solutions provide both the ease and simplicity of SaaS and the manageability required to respond quickly to shifting business needs.

PKI at Enterprise Scale. Microservices architecture, containerization and DevOps toolchains all increase the number of TLS connections that need to be managed by an internal PKI. The deployment of millions of IoT devices have added many more. Using TLS to secure worker endpoints, mobile phones and network devices has added even more. Together, all of these changes have dramatically increased the scale of challenges PKI teams must solve. PKI that was designed and deployed 10 years ago just can't keep up anymore. A new approach is needed.

The Solution: Venafi Zero Touch PKI

The best way to take the pain and risk out of internal PKI is to hire experts to do the job for you. The Venafi Zero Touch PKI solution is a robust, flexible and highly secure solution that addresses your pressing private PKI needs—while requiring almost no time or effort from your own InfoSec staff. It also doesn't require an army of consultants and a hefty services budget.

A Fully Managed, No Hassle PKI Service. Venafi Zero Touch PKI is fully managed by experts on the Venafi staff. Your modern PKI is built to your specifications, leveraging the CAs, roots and intermediaries needed by your business. Each customized PKI is designed with current best practices for design, deployment and security in mind, ensuring your PKI leverages the latest capabilities and protocols.

SaaS-Based, Cloud Hosted PKI. Your InfoSec team will have complete API- and GUI-based access to the hosted solution, allowing them to change configurations when needed or execute custom tasks.

But unlike your old PKI, you don't need to set up your own servers, configure requests, validate functions, upgrade databases and monitor connections (and repair them if they go offline). Venafi Zero Touch PKI gives you the customization modern PKI solutions require, but with a high degree of ease of use and rapid time-to-value.

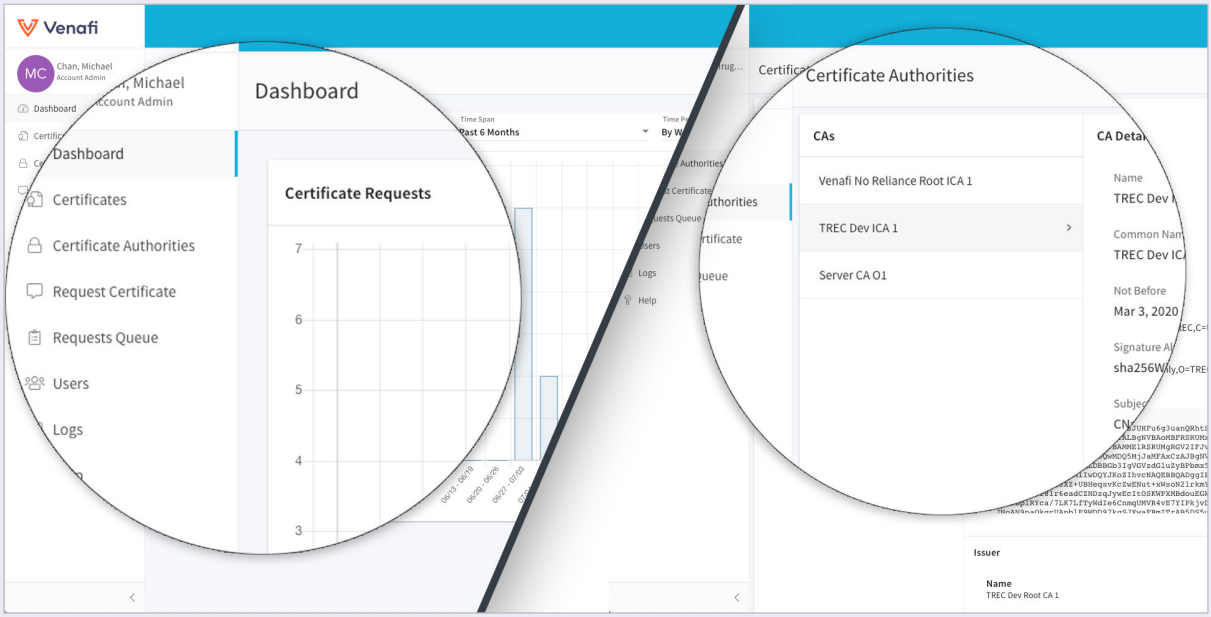
Security Controls and Best Practices Built-In. Industry best practices for PKI and Trust infrastructure are constantly evolving. Every Venafi Zero Touch PKI is implemented with modern best practices for security and control, including infrastructure that's fully air-gapped and never online, along with key generation and storage in a DoD-spec, vaulted, granite-protected facility.

Ready-Made Certificate Issuing Profiles. Certificate issuing profiles are critical tools that can make or break your private PKI. These profiles configure the content for TLS certificates, establish security constraints, and define input and output forms for certificate enrollment. Venafi Zero Touch PKI includes profiles for cloud-native processes as well as for mobile, telephony and network devices. These templates dramatically simplify your private PKI solution without sacrificing security or functionality.

Auto-Enrollment Ready. In today's threat landscape, all systems are critical systems, not just web servers and app servers. Microsoft Active Directory Certificate Service (ADCS) allows Microsoft servers and devices in your organization to automatically enroll for TLS certificate coverage. Auto-enrollment automates a labor-intensive process, and by integrating with it, Venafi Zero Touch PKI makes sure the largest portion of your IT estate doesn't go without the protection TLS certificates provide.

Instant Integration with Venafi Trust Protection Platform. Venafi customers rely on the Trust Protection Platform to provide visibility, intelligence and automation for TLS certificates all the way down to specific hardware, application and workload levels. Zero Touch PKI comes with out-of-the-box integration to the Trust Protection Platform, providing an end-to-end solution that automates the machine identities your business relies on.

Venafi Zero Trust PKI – Dashboard view (left) and Certificate Authorities view (right)



How It Works

Venafi Zero Touch PKI is a hosted, fully managed SaaS service that lets your InfoSec teams focus on external, public-facing systems while your internal, private PKI needs are met by a trusted, automated and cloud-based solution.

Zero Touch PKI	
PKI Features	• Flexible root and intermediate CA hierarchy configuration • RSA and ECDSA CA and certificate issuance • Offline root key custody management • Management of online issuing CA(s) signing, operations and documentation • Offline and online key material BCP and disaster recovery process • Management of all certificate validation processes, including HA implementation and highly scalable OSCP and CRL processes • HSM operations and HA model for continuous operations • Web-based certificate management portal • Ongoing secure operations of all online issuing CAs in FIPS 140-2 level 3 hardware • Automation for MS autoenrollment and other standards-based certificate management protocols such as SCEP, EST and ACME, as well as API support • Design and implementation of private trust hierarchy architecture(s) • Turnkey root key generation ceremony processes and documentation
Service and Support Features	• Guidance and support for current PKI migration to the Venafi managed service, as well as guidance and recommendations for migration of CA key material obtained in acquisitions • 99.9% availability and uptime • U.S. and European data center operations • 24x7x365 availability, support, security monitoring
Integrations and Services	• **Mobile Device Management:** Microsoft Intune, Airwatch by VMWare, MobileIron, Citrix ZenMobile, Jamf Now, Jamf Pro and more • **Microsoft Auto-Enrollment:** Windows desktops. servers and laptops • **Network and IoT Enrollment:** SCEP (Simple Certificate Enrollment Protocol) and EST (Enrollment over Secure Transport) • **Applications and Developers:** ACME2 for cert-bot and more integrations; complete REST API • **Venafi:** Native, built-in integration with Venafi Trust Protection Platform

Next Steps

Does your organization need to replace outdated systems, expand your PKI to meet new security needs or support new sites and services for remote workers? Venafi Zero Touch PKI can help. Get a consultation with a PKI expert or visit **venafi.com/platform/zero-touch-pki/consultation**

Venafi is the cybersecurity market leader in machine identity management, securing the cryptographic keys and digital certificates on which every business and government depends to deliver safe machine-to-machine communication. Organizations use Venafi key and certificate security to protect communications, commerce, critical systems and data, and mobile and user access. **To learn more, visit venafi.com**