Buyer's Guide

Buyer's Guide for Certificate Management

How to choose a certificate management solution that maximizes flexibility, control and security

Organizations like yours are grappling with a tsunami of new keys and certificates necessary to support privacy regulations, DevOps projects and IoT devices. These high value security assets are used to identify and authorize machine-to-machine connections and communication, making them high value targets for cyber attackers and malicious insiders.

As certificate counts within the average organization rise to tens of thousands, it has become exponentially harder to manage them effectively. Many organizations turn to their certificate authorities (CAs) to protect the keys and certificates that each CA issues. The basic tools CAs provide are certainly a step up from manual or homegrown methods many organizations use, but do they provide enterprise-wide protection for your machine identities?

Whether avoiding outages of critical services or protecting machine identities from the cyber criminals who target them, you need certificate management that delivers security, availability, and reliability. We've compiled a security checklist to help you select the most effective key and certificate orchestration solution for your organization.

Maximizing CA Agility

- **Does your organization need the flexibility to rely on more than one CA?**

  Most organizations use multiple CAs, but it's not possible to manage multiple CAs using a single CA management console. This means a holistic view of all your organization's keys and certificates will require ongoing manual effort to consolidate this information, which is error prone and time consuming.

- **Does your organization need the ability to change, remove or add a CA quickly?**

  Most organizations need to be able to respond quickly if a CA implementation is compromised through unauthorized access or corrupted due to lost keys. The ability to switch CAs easily offers a critical security advantage. In addition, many organizations prefer not to be locked in to a specific CA vendor because it limits business agility and can incur additional expenses.

- **Do you find it challenging to ensure all your keys and certificates comply with corporate security policies?**

  With CAs only managing the certificates they issue, to get consistent policy enforcement, you'll either need to consolidate all your keys and certificates onto one CA or repeat the implementation of security policies across multiple CAs. In addition, with multiple CAs, you won't be able to automate enforcement of security policies across the various CA certificate management solutions.

- **Can you maintain consistent security across all keys and certificates?**

  Most certificate users generally don't understand how to provision strong keys and certificates. They often revert to older, more familiar issuance practices, which may be based on less secure configurations. Also, odds are, you won't be able to limit certificate issuance to your policy-approved CAs.

  Recommendation: Choose a solution that will give you ultimate flexibility in actively managing all your certificates from a single console. You won't tie your organization's security posture to any single CA vendor. Plus, you'll be equipped to implement consistent security policies across all CAs and deliver audit-ready reports and documentation about your company-wide key and certificate management program. You'll also be able to add, remove or change CAs at a moment's notice without impacting your security posture or the availability of critical applications or services.

Accelerating DevOps

- **Does your organization have a DevOps team or project?**

  Motivated by compressed timelines, DevOps teams often rely on ad hoc provisioning. Plus, they may resort to reusing keys and certificates, or skip using them all together. To meet Service Level Agreements (SLAs), they often generate their own keys and certificates, using PKI implementations like OpenSSL, Dogtag or Let's Encrypt that violate most enterprise certificate policies and introduce unnecessary security risks.

- **Do you have the agility to support the speed of DevOps?**

  Not all CA certificate management solutions are flexible enough to support the speed and agility requirements of DevOps. Plus, they may not be tightly integrated into DevOps platforms to allow DevOps teams maximum flexibility while ensuring compliance with security policies. And, once DevOps code moves to production many organizations need the agility to consolidate or replace CAs.

  Recommendation: To avoid the inefficiencies of traditional provisioning in a DevOps environment, look for management and security solutions that offer in-depth integration with DevOps platforms, such as Chef, Puppet and Docker. Make sure this is complemented with the automation needed to ensure consistent security without slowing DevOps delivery. Choosing a solution that works with any CA will allow you to manage DevOps keys and certificates at the same high levels of security that you enforce across the enterprise.

Reacting Quickly to Security Events

- **Can you respond quickly to a CA compromise?**

  If you rely on a single CA to issue and manage your certificates, you'll face a world of pain if that CA is compromised. Unfortunately, this is not an infrequent event. And when it happens, it leaves many CA customers scrambling to find another CA and to convert all their keys and certificates. Plus, any automated processes, integrations with security infrastructure and policies that were developed using the compromised CAs will need to be rewritten.

- **Can you identify and react quickly to an outage or breach?**

  If you rely on multiple CAs and don't have enterprise-wide awareness of your key and certificate security posture, you will be unable to respond quickly to a misused certificate, an unplanned outage or a vulnerability. And when you're experiencing an outage or a breach, time is critical. The longer the outage or breach continues, the greater the potential damage to your organization.

  Recommendation: Don't get locked into any provider for your keys and certificates. Look for a centralized, CA-agnostic management solution that gives you the agility to rotate, replace and revoke all impacted keys and certificates across any CA or switch out all certificates from one or more CAs when needed. This approach will also allow you to add, change, consolidate or remove CAs quickly and easily. Choose a CA-agnostic platform that leverages APIs across numerous CAs, so you can easily apply your current key and certificate policies across CAs.

Integrating with Your Infrastructure

- **Do you integrate keys and certificates with your security and network infrastructure?**

  It's one thing to make keys accessible to network and security applications, but it's quite another to do it easily. With multiple CAs issuing certificates in your environment, you'll quickly run into challenges implementing them with applications.

- **How often do you add new applications to your infrastructure?**

  In today's evolving networks, you will need to integrate with the latest technologies. CAs lack "adaptable" integration capabilities that allow you to easily extend access to keys and certificates by any application in your environment.

  Recommendation: It is important to make sure that the platform you choose comes with a full suite of pre-packaged integrations. This will help you quickly automate and scale the distribution of keys and certificates to encryption-dependent applications. Plus, a well-documented API that features "adaptable" integration capabilities will allow you to easily extend near real-time key and certificate access to all custom and legacy applications in your environment.

Centralizing Key Generation

- **Do you have a centralized repository and management for your keys and certificates?**

  Without a central repository and centralized management for all keys, it's difficult for organizations to enforce strong key generation—leaving users to make their own choices from a bewildering set of options.

- **Can you deliver real-time access to keys and certificates for SSL inspection?**

  Real-time SSL/TLS inspection can allow encrypted traffic to be decrypted, inspected and re-encrypted to detect threats without delaying communications. But this only works if your organization can deliver real-time access to SSL/TLS keys, which will need to be shared with multiple applications.

  Recommendation: If these issues are important to you, then you should choose an orchestration framework that has access to application keys. Look for a solution that centralizes key generation, management and storage as this is the only way to facilitate distribution to multiple endpoint applications.

Choose the Best Management for Any CA

Keys and certificates are used throughout your network to protect machine-to-machine connections and communications. Enterprises often have to manage tens of thousands of these critical security assets. Don't get locked in to a single certificate authority that will limit your business agility. Choose a solution that provides your organization with the maximum flexibility so you can proactively manage your keys and certificates. Then you can take advantage of the redundancy and resiliency of using multiple CAs to secure machine identities and communications in your organization.

About Venafi

Venafi is the cybersecurity market leader in machine identity protection, 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 www.venafi.com

Part number: 161123-BG-CertManagement