Buyer's Guide: Maximize Agility Across Certificate Authorities

How to manage certificate authorities to maximize security, flexibility and control

Today's organizations are challenged by an explosion of machines on enterprise networks, as well as a corresponding increase in encrypted network traffic. To support this dramatic increase in encryption, your organization will need tens of thousands of cryptographic keys and digital certificates to serve as identities for machines that enable encryption, decryption and authentication. To acquire these certificates, organizations generally establish and maintain trust relationships with at least a few external certificate authorities (CAs).

Experts now recognize the importance of crypto-agility in maintaining successful CA implementations. Crypto-agility is the ability to replace encryption certificates and keys quickly in response to security events or business needs, particularly when bulk replacement is needed. CA-agility is a critical component of crypto-agility, enabling incident response to issues with one or more CAs. To achieve CA-agility, enterprises need to architect their CA relationships and certificate management infrastructure to support agility across internal and multiple external CAs.

Unfortunately, relying on CA-specific management tools prevents enterprise-wide certificate visibility and management. CA tools only manage certificates issued by that CA and don't have information about where certificates are installed or who owns them. It's far more difficult for IT and security teams to react quickly to a CA incident if solely relying on CA tools.

To cope with this complexity, you need a flexible, CA-agnostic approach to certificate management—one that adapts easily to your business needs and environment, while also enabling you to respond to external CA issues. To help you find the best solution for your organization, we've compiled a checklist that will help you maximize security, availability and reliability across all CAs used by your organization.

Maximizing Visibility and Control for CA-agility

- **Do you have a complete and accurate inventory of every certificate in your organization?**

  Like most organizations, you probably use more than one CA. But relying on CA management consoles only gives you a partial view of the certificates used in your organization. To gain a holistic view, you may resort to manual methods, which can be error prone and time consuming. Look for a CA-agnostic solution that automates the discovery of every certificate used in your expanded network.

- **Can you actively monitor all certificates to uncover day-to-day changes?**

  It's one thing to build an inventory, but it's a different thing altogether to keep that inventory fresh every day. You need to know where each certificate in your inventory is installed and whether it has changed. Certain changes, such as a CA error that invalidates multiple certificates, will require immediate attention. Look for a system that continuously monitors all your certificates, regardless of the issuing CA, so that you can act quickly when required.

- **Can you quickly locate and replace a single certificate or group of certificates?**

  If you're relying on CAs to manage your certificates, you won't have the intelligence you need to rapidly respond to a CA breach or error. CAs can provide basic information about certificates, but to act quickly you need to know every location where a certificate is used and who manages that device or application. So, for CA-agility, you can't rely solely on CA certificate management. Instead, look for a solution that delivers this crucial certificate intelligence on location and ownership.

- **Do all your keys and certificates comply with corporate security policies?**

  Because CAs only manage the certificates they issue, consistent policy enforcement can be problematic. If relying on CA management consoles, you'll either need to consolidate all your keys and certificates onto one CA or try to implement the same security policies across multiple CAs, each of which may handle security requirements differently. Look for a solution that gives you the flexibility to set and enforce your organization's security policies uniformly across all certificates and all CAs in your environment.

- **Can you find certificates from unauthorized CAs?**

  Some certificate users in your organization may install certificates from free or low-cost providers to support new business initiatives or rapid deployment requirements. In order to find rogue certificates, look for a solution that gives you a comprehensive view of all certificates in use, including those in the cloud or used by third-party partners, regardless of the issuing CA.

Reacting Quickly to Security Events

- **Can you change, remove or add a CA quickly in the face of a CA compromise or error?**

  If a CA can no longer be trusted because of unauthorized issuance, lost or stolen keys or any other reason, you need to be able to respond quickly. To replace a CA, you must be able to locate all impacted certificates, then reissue them from another CA. Look for a CA-agnostic solution that makes it possible to automate the removal of impacted certificates and the installation and validation of new certificates.

- **Can you respond to browser distrust of a CA?**

  If you rely on CAs to manage all your certificates, you will limit your options if one of your CAs is distrusted. This is not an infrequent event. Browser makers are taking a much more active role in policing the level of trust earned by CAs. When CAs are distrusted, many customers must scramble to find another CA and to replace all their keys and certificates from the distrusted CAs. Look for a certificate management solution that enables the automated replacement of keys and certificates in bulk to transition to a new CA quickly.

- **Can you seamlessly transfer policies and integrations to a new CA?**

  Each CA management tool may apply policies and integrations differently, complicating a transition between CAs. Look for a certificate management solution that doesn't require you to rewrite any automated processes or integrations with security infrastructure and allows you to reuse security policies and workflows when switching CAs.

Aligning CA Use with Your Infrastructure

- **Are you using the right CA for the job?**

  You may want, or need, to use different CAs for different business functions. But with multiple CAs, you'll quickly run into challenges integrating your various CA certificate issuance and management approaches with your security and network infrastructure applications. Look for a certificate management solution that works with any CA to install certificates on leading network and security applications.

- **Is your certificate life cycle automated with each CA?**

  No one wants to manually copy and install all the required files from different CAs across the network. Automatic installation prevents errors and saves precious IT resources required to transport the keys securely

and install them correctly. Ideally, you want one certificate management solution that automates the entire certificate life cycle—regardless of the CA used. This should include issuance, installation, renewal and validation. With life cycle automation, you'll avoid the ongoing cost and burden of touching every encryption-dependent application every time a key or certificate is changed.

- **Are your alerts and notifications from different CAs helpful or just noise?**

  When relying on different CA management tools, you can receive alerts and notifications from each of these tools, but they won't coordinate and prioritize communications across your key and certificate environment. Look for a certificate management solution that proactively reaches out to other systems to orchestrate communications from all CAs. Programmable software hooks should allow your solution to automatically respond and take action when specific conditions exist. Then, when an event occurs that requires immediate and appropriate action, it will be appropriately prioritized and escalated.

- **Can you easily integrate certificate issuance from different CAs to various applications?**

  In today's evolving networks, you will need to integrate encryption with the latest technologies. This includes dynamic technologies, such as cloud and DevOps platforms. And the ability to integrate certificate issuance with certain applications may be limited to particular CAs. Without consistent, yet adaptable, integration capabilities across CAs, integrating certificate issuance becomes cumbersome, if not outright impractical. Look for a well-documented API that provides adaptable integration capabilities that will allow you to quickly and easily extend key and certificate issuance and access to all custom and legacy applications in your environment—supporting your current CAs and any you may add in the future.

Take Control: Optimize for CA-agility

Keys and certificates are used throughout your network to serve as machine identities and authorize and protect machine-to-machine connections and communications. Don't get locked into a single certificate authority that will limit your business agility or get stuck with disjointed management across CAs. Choose a solution that delivers the flexibility to use various CAs based on business need and allows you to proactively manage your trust model to protect your company, your customers and your partners. You'll have the CA-agility to make changes at a moment's notice without impacting your security posture or the availability of critical applications and services.

CA-agility Checklist

A CA-agnostic platform for certificate management and security will help you avoid the limitations of being locked in to a single vendor or the impacts of mismanagement across multiple CAs. Look for the following capabilities:

- Comprehensive discovery to create an accurate inventory across CAs
- Centralized management across CAs to actively manage all certificates from a single pane of glass
- Global intelligence to respond quickly to security events and changes in internal and external requirements
- Intelligence-driven automation to issue, rotate, revoke, replace and validate keys and certificates across any and all CAs
- Adaptable integration options that easily integrate machine identity intelligence access with any application

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