White Paper

Seven Tough Questions Every Brand Should Ask Before Switching Certification Authorities (CAs)

Key Considerations for a Simple Migration

ENTRUST

SECURING A WORLD IN MOTION

Table of Contents

INTRODUCTION

Taking the matter of choosing a certification authority (CA) into your own hands is a wise move, and it's fortunately not as challenging as you might think.

Transitioning any element of an organization's IT infrastructure is a serious consideration given the impact it can have on systems, security, and overall efficiency. Sometimes the established protocol only seems best or efficient because it's familiar. The CA responsible for the issuance and management platform of the digital certificates that secure internal servers, web applications, emails, and other security protocols definitely deserves the scrutiny of a watchful IT team.

Transitioning digital certificates over to a new CA introduces uncertainty to key touch points such as IT infrastructure and security, customer privacy, websites, and e-commerce. These touch points warrant considering whether your current CA can adequately provide brand security for your organization and the customers who transact on your website.

Several events can trigger the need to migrate over to a new CA, including whether a CA:

- **Adequately protects your brand**
- **Follows CA/Browser Forum guidelines and best practices**
- **Offers pricing and licensing policies that meet your budget objectives**
- **Can grow with your organization and meet all of its current and future needs**
- **Actively participates in the CA Security Council and supports initiatives that mitigate security threats**

This white paper discusses the seven tough questions and key considerations that should be assessed before transitioning to a new CA. It also demonstrates that migrating digital certificates over to a new CA is a fairly straightforward process.

The Seven Tough Questions

There are seven key questions that need to be answered when interviewing new CAs in preparation for a migration. These key considerations will make the transition simple and complete and probably leave you wondering why you waited so long to make the switch.

1. What is your approach to our organization?

As industry experts, the CA should take a consultative approach to the project, working in partnership with the various stakeholders in your organization to achieve the mutual objectives of a seamless integration from the current CA to the new one. They should establish a workflow process for certificate management that meets the organization's unique business requirements.

- **ESTABLISHING TEAMS AND IDENTIFYING RESPONSIBILITIES**

  The new CA should be willing to meet with your team(s), including executive- and director-level personnel in IT, IT managers, and any cryptographers who will manage the day-to-day activities, finance, and procurement, and any other key stakeholders who deserve a seat at the table in the decision-making process. Meet with and identify the team members from each organization, detailing who the contact people are and their specific responsibilities.

- **UNDERSTANDING THE BUSINESS**

  Understanding your business is an essential component of a successful partnership. Consider how much experience the new CA has in serving your industry, the size and geographical scope of your organization, and how well they demonstrate any related and transferable experience.

- **UNDERSTANDING UNIQUE BUSINESS REQUIREMENTS**

  Each organization has its own unique business needs, and the new CA should be able to demonstrate how their platform and protocols can either meet or improve upon existing needs — as well as how they are poised to accommodate growth and future requirements.

- **ESTABLISHING A FEASIBLE PROCESS**

  The new CA should establish a specific process for achieving your goals and create a feasible timeline that drives toward those goals.

- **DEMONSTRATING ABILITY TO MAINTAIN SECURITY AND ACHIEVE GOALS**

  Conversations are great at breaking the ice, but it's important to observe the actual activity that proves the new CA's level of commitment and willingness to go above and beyond to avoid business disruption and maintain strict security protocols.

2. How will our communicated concerns be addressed?

The new CA should thoroughly understand your concerns and have a cohesive plan as to how to mitigate risks and achieve a seamless migration. Most organizations are concerned with five main categories:

- **INVENTORY**

  Capturing the full inventory of digital certificates across a globally distributed enterprise is a major concern for enterprise organizations. The new CA should be able to demonstrate the search and importing tools that they have available to find certificates across multiple platforms and variant ERPs and centralize visibility to one certificate lifecycle management platform. The best tools have discovery, certificate transparency (CT) search, CT import, and manual import capabilities.

  CT search gives you a tool to review who has issued TLS/SSL certificates to your domain name. It helps prevent interception by impersonators and identify the issuance of TLS/SSL certificates by rogue CAs.

- **ISSUANCE AND INSTALL**

  Expediency and accuracy are critical to establishing trust between the new CA and your organization — and between your organization and the people and systems who engage with them.

  Requirements for issuing OV and EV certificates should be communicated upfront to avoid hiccups and maintain established turnaround times.

  Auto installers can significantly increase the speed and accuracy with which TLS/SSL certificates are deployed. Automated controls take the burden of manual processes off IT resources. This decreases overhead costs, mitigates risks, and reduces the need to take servers down, among other time-consuming troubleshooting efforts.

  Auto installers, coupled with automated renewal on pre-approved domains, also remove the risk of expired certificates, providing more uptime for web applications and servers.

- **COSTS**

  Costs can vary significantly among CAs, and you should look beyond face value to consider everything that's included with a certificate. Flexible licensing policies (e.g., an automated subscription plan, certificate management capabilities, unlimited server licensing, and unlimited reissues) provide significant savings.

  An automated subscription plan is a budget-friendly plan that allows for decommissioned licenses to be reused and can provide tremendous savings in environments where certificates are used on a short-term basis for testing or load balancing, for example. An automated subscription plan eliminates the friction caused by manual reconciliation reports, which are prone to error and time consuming.

- **MAINTAINING VALIDITY**

  Leaving behind the active life remaining on existing certificates during a transition can be a concern for organizations that have already invested in a significant inventory. Many CAs are happy to work out a plan that honors all or part of the remaining validity period for a specified amount of time. An arrangement like this can ease budget constraints.

- **SECURITY**

  Ensuring and maintaining secure web applications for customers and internal data transmissions should be an organization's paramount concern. This is an area where the new CA should prove an ongoing commitment to meet or exceed industry standards and regulations to protect brands and the people who transact with them.

- **INDUSTRY STANDARDS**

  Industry Standards Groups
  Evaluate the new CA's relationship with industry standards groups. Research their history with meeting the baseline requirements that were established by the groups to maintain a secure certificate population for public trust. All CAs are required to undergo and pass an annual audit.

  Security in Practice
  Identify the practices the new CA has in place to maintain strict security protocols and risk mitigation to optimize security for your organization including server configuration testing, best practices, ongoing customer training, and education.

  Voluntary participation in efforts that stem the surge of known threats can be more impactful when done as a collective effort to maintain a secure IT ecosystem for public transactions. What is the new CA's position on this? What tools and systems are in place to mitigate risks from phishing attacks?

3. What level of support will you commit to our migration project?

- DEDICATED RESOURCES

  The new CA should be willing to identify and dedicate key support specialists to a large-scale CA migration project, including contact information with the ability to reach them outside of business hours:

  • One-to-one customer relationship
  • Technical support expert(s)
  • Installation support
  • Verification specialist(s)

- PROJECT TIMELINE

  The completion of CA migration projects is predicated on several factors and varies in length based on company size, number of domains, and the types of certificates being deployed. Once the contingencies are established, the new CA should be able to deliver a feasible timeline in which to complete the migration.

4. Can you detail for us the performance level of key technology impacted by the migration?

- ROOT UBIQUITY

  A CA's root certificates are the foundation of trust — ensuring your users and brand are trusted globally. Root certificates are the first link in the chain of trust. Web browser and connecting devices inherently trust all certificates that have been signed by any root that has been embedded in the browser itself or in an operating system on which it relies.

  A mature CA who has been embedded within the root programs for a vast period of time will have the ability to add greater ubiquity, even for newer roots. This is done by re-chaining the new roots to their older legacy roots. This is key to ensuring that legacy nodes/devices that do not receive root program updates will trust your new CA.

  You must ensure your new CA has the ubiquity to meet the needs of your users and customers.

- **COMPLEX CHAINING**

  Industry protocol requires CAs to utilize a chain of certificates stemming from a trusted root. This process, also known as complex chaining, mitigates risk, improves performance, and offers a CA flexibility in establishing policy.

  Certificates that are chained to the root are subordinate to it and offer it a veil of protection in the event of compromise. The compromise would only impact up to the chained certificate protecting the trusted root. Verifying revoked certificates can be done more expediently because the certificate revocation lists (CRLs) only roll up as far as the certificate it's chained to.

  CAs can strengthen certificate chains by establishing newer policy and encryption protocols that improve security. Even though a trusted CA is listed in the root programs, your organization might have decided to have tighter security and enforce a select number of CAs to be trusted (e.g., internal and current public CA). This is done through network policies.

  - Check to make sure that there are no custom trust lists of roots enforced through network policies on your internal network.
  - Check to ensure that there are no third-party services that enforce this as well. You might need to submit a service request to add a new CA to your third-party's trust list.

  A reliable CA can show you their ability to provide multiple paths of trust through complex chaining. Issuing end-entity digital certificates directly from the root CA introduces risk, limiting how certificate policy can be managed and enforced.

- **ROOTS RECOGNIZED BY THIRD-PARTY SOFTWARE**

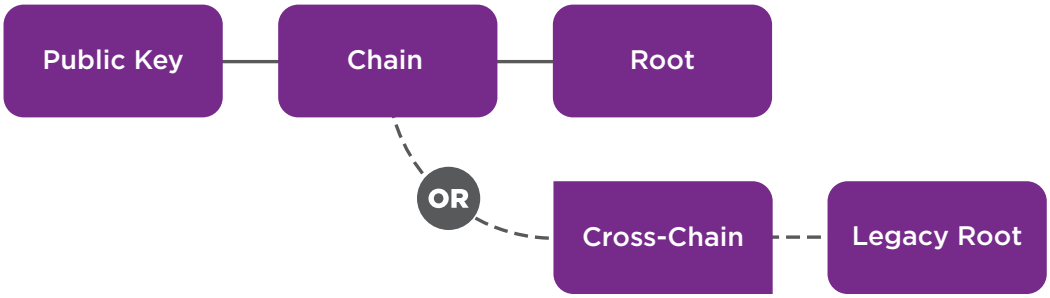
  A CA's roots must be trusted for applications involving server-to-server communication. In addition to browser ubiquity, a CA's roots must be accepted by an organization's IT infrastructure

- **CERTIFICATION AUTHORITY AUTHORIZATION (CAA)**

  CAA enables domain owners to specify within their DNS records the CA that is authorized to issue certificates for the specified domain. The new CAA policy has been defined by the CA/Browser forum and has been in effect since Sept. 8, 2017.

Hierarchy of Trust

Example of a path of trust that allows the use of multiple roots:



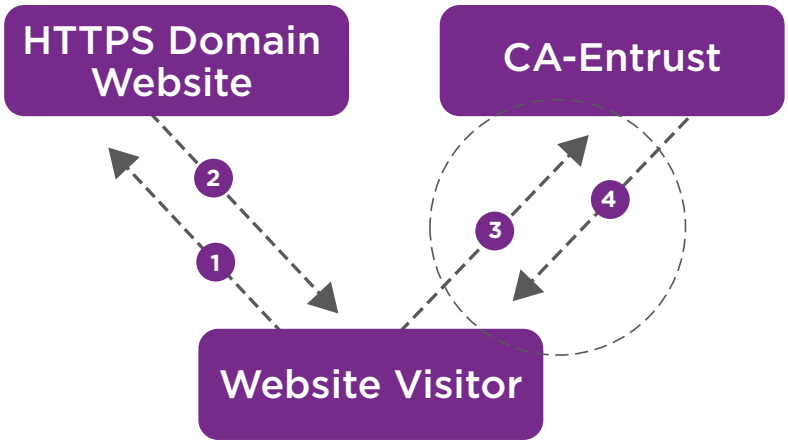
The technical requirements for CAA are covered by standard RFC 6844.

- CAA tightens security for domain owners by enabling them to limit certificate issuance to only those CAs they have granted permission to — this can be either none, one, or many specific CAs. CAA can also grant permission for wildcard certificates. This allows a specific CA to issue wildcard certificates or completely prevent the issuance of wildcard certificates for the domain.
- CAA may be the best way to protect domain owners from having fraudulent certificates issued in their domain name. This has become increasingly important with the proliferation of unauthorized domain validated (DV) certificates.
- CAA record checking is mandatory for all CAs but voluntary for domain owners. It is a great benefit for domains to register approved CAs to prevent fraudulent certificates from being issued to your domains.
- Before deploying a CAA record, identify your current trusted CAs. This can be done by performing a CT search or by using a certificate discovery tool. Once CAs are identified, deploy CAA records for all CAs you plan to continue using.
- If you use a hosted DNS service, follow these links for instructions on how to add a CAA record to your DNS zone file and how to add a CAA record in a hosted DNS.

Organizations should look for a CA that supports and abides by CAA policy.

- **WEBSITE PERFORMANCE**

  The amount of time it takes for the browser to validate a TLS/SSL certificate is critical for busy end-users who don't like to wait for pages to load. This makes communication time between a website and CA a critical component in the decision-making process.



1. Visitor hits website.
2. Website returns certificate. Browser checks validity (date) and trust (is root in browser).
3. Browser checks for revocation status with CA.
4. CA returns a yes/no response.
5. Website completes rendering.

The average OCSP response time should be under 80 milliseconds (ms) for end-users to have a seamless experience.

5. What is your verification process, including requirements and turnaround times?

The CA/Browser Forum is an industry standards group that creates the guidelines all CAs must adhere to for digital certificate issuance. The process and requirements are the same for every CA. This means that whether you're purchasing an organization validated (OV) certificate or an extended validation (EV) certificate, the verification process and requirements should not differ between the CAs.

Look for distinctions in the level of service offered and anticipated turnaround times for issuing certificates:

Level of Support

A large enterprise should be able to request that a dedicated verification specialist overlook the entire transition effort, providing a single point of contact.

Turnaround Time

The average turnaround time for new domains and organizations verified to the OV standard is one to three business days. Where verification is carried out to the EV standard, the average turnaround time is three to five business days. Instant issuance of EV and OV TLS/SSL certificates should be available for pre-verified domains and organizations.

Hours of Availability

A global team that is strategically distributed worldwide can offer the most complete coverage and should be available 24x5 Monday through Friday to assist you. Most CAs offer a higher level of service, including extended hours (24x7x365) and faster turnarounds as an additional offering.

Contact Methods

Multiple support outlets, including phone, email, and chat, should be available to provide the most expedient communication method for the organization's resources.

Dependencies include the response time from members of your organization's team in getting requested information and phone validations returned expediently.

Here is a quick overview of the verification requirements for OV and EV certificates:

OV CERTIFICATE

- Show control of domain
- Location
- Proof of an active and registered business
- Evidence of a physical location
- Third-party telephone number to validate call
- Employee contact (or someone who manages certificates on behalf of the contact)

EV CERTIFICATE

- In addition to the OV requirements, EV certificates require these additional checks:
- Jurisdiction information
- Where the business is incorporated
- Additional contacts:
  - Contract signer
  - Higher authority (director level or above; or if a manager, they must supervise the requesters)

6. Can we schedule a comprehensive demonstration of your Certificate Management platform? And, is there a trial account available for our team to experience the platform?

Before engaging with prospective CAs, work with the hands-on resources in your organization who are responsible for tracking expirations and the day-to-day management of digital certificates. Identify what capabilities the new CA must have as well as what you would like to have that isn't currently available. Ask the prospective CA to demo these features and to show you any unique or innovative functionality on their platform. In addition, inquire about enrolling in a trial version where your IT staff can get hands-on experience with the platform.

- ### CENTRALIZED MANAGEMENT CAPABILITIES

  Connect the tools and processes that are available on your existing platform with those you will need to secure and manage your complete digital certificate inventory on the new platform. Think about some capabilities that are not available with your current CA but would enhance certificate management, and inquire whether the prospective CA already has those capabilities.

- ### CONSOLIDATED CERTIFICATE MANAGEMENT

  Organizations that use digital certificates from more than one CA need the additional visibility to manage the entire digital certificate inventory enterprise-wide, from a single platform. Tools like discovery, CT import, and manual import are essential to this process.

- **DELIVERY METHODS**

  Automated installation tools and various certificate delivery options remove the challenges of error-prone manual processes and speed up the installation process.

- **COMPLIANCE AND BEST PRACTICES**

  Applying best practices involves both providing the tools and the ongoing education that ensure secure endpoint configuration, visibility, threat prevention, and preparedness to secure domains against new and emerging threats.

- **REPORTING AND ALERTS**

  Critical components of digital certificate management include the ability to maintain uptime for web applications and staying apprised of expiration dates with certificate inventory management.

- **BUDGETING AND PLANNING**

  Flexible licensing policies, budget-friendly subscription plans, and certificate swap capabilities can provide cost savings and value that extend beyond the face value of the certificate itself.

- **SUB-ADMIN DELEGATION**

  Simplifying certificate issuance and centralizing the budget for digital certificates across a large enterprise become practicable when the system allows for groups within an organization to have responsibility for just a portion of the overall certificate inventory.

- **WEBSITE SECURITY BUNDLES**

  A website security bundle that identifies malware and common website vulnerabilities, allows for scheduled and on-demand scans, provides reputation monitoring, and offers options for remediation serves a more complete digital security package to your organization if there is not already one in place.

- **ONE SOURCE FOR ALL CERTIFICATE TYPES**

  Having a wide range of digital certificate types such as TLS/SSL, code signing, document signing, S/MIME, and devices available through a single certificate management platform offers you the easiest administration.

7. Do you have the capabilities to create customizable workflows and integrate with the third-party vendors that we use regularly to manage our workflow?

The CA should be able to provide web forms that scale to any business size and can be embedded into the workflow process to conform to the organization's unique business needs. E-forms and APIs are common tools that enable a CA to distribute roles across an organization. For example, TLS/SSL subscribers can make certificate requests, relieving PKI administrators of tedious responsibilities. These tools help achieve a seamless integration that fits into the existing business model.

Third-party integrations are a crucial consideration for enterprises looking to maintain a centralized system for workflow processes. A CA that has experience integrating with platforms such as Venafi and ServiceNow, or any other API integration, can really help facilitate a smooth transition.

Migration Checklist

ACTION	CUSTOMER	CERTIFICATION AUTHORITY
Set up POC	X	X
Provide domain list (using CT search and discovery)	X	
Provide company name list	X	
Validate domains		X
Validate company names		X
Admins and roles list	X	
Validate admins	X	X
Delegation setup	X	X
Inform TLS/SSL subscribers of CA migration	X	
Distribute Intermediate certificates for new CA hierarchy	X	
Maintain list of certificates to be migrated	X	
Establish policies (e.g., certificate expiry notifications, recipients, and escalation procedures)	X	
Create customized certificate request & approval workflow (e-forms)	X	X
Venafi integration	X	X
ServiceNow integration	X	X
Training		X

Conclusion

Identifying your needs and measuring them against what a prospective CA can deliver removes the uncertainty surrounding the CA migration process. It can go a long way in giving your organization the confidence to move forward with a transition to a new CA that has the capabilities and reputation your organization needs to strengthen customer engagement.

Change is often in the best interest of the organization when it is well thought out and contributes to the overall strategic value of the organization. Migrating to a new CA can create greater brand security and bring peace of mind to the IT team who protects the brand and to the customers who rely on your organization to secure their online transactions.

For more information

888.690.2424
+1 952 933 1223
info@entrust.com

entrust.com

ABOUT ENTRUST CORPORATION

Entrust secures a rapidly changing world by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

ENTRUST

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com