Key Considerations when Choosing or Switching a Certificate Authority

TLS/SSL certificates are vital to encrypting critical data

Internet security is a necessity and a priority when organizations offer online services, transactions, logins, and contact forms. TLS/SSL certificates are utilized to keep the end-users' information safe while in transit, and to verify the website's organization identity to make certain users are interacting with legitimate website owners. TLS/SSL certificates are a vital element to encrypt critical data – most global organizations have more than one certificate authority (CA).

Why would you need to choose or switch to a CA?

Choosing the CA that fits your organization's use cases is important. Not all CAs provide the same service or can work with your existing IT infrastructure, customer privacy, and security requirements. Whether you are looking for an additional CA or need to switch your current provider, these are some key questions to ask to help validate your choice of solution:

KEY QUESTIONS

1. Does the CA adequately protect the brand?
2. Does the CA follow CA/Browser Forum best practices and guidelines?
3. Does the CA offer flexible licensing and pricing policies that meet your budget and business needs?
4. Can the CA grow and scale with your organization to meet current and future needs?
5. Does the CA actively participate in the CA Security Council and support initiatives that alleviate security threats?

Learn more about our digital certificate solutions at entrust.com

Successfully onboarding a CA

How do you choose or switch a CA for TLS/SSL certificates?

There are several key factors to consider when choosing or switching a CA:

1. Does the solution integrate with your existing IT infrastructure?
2. Can the solution meet your growth and scalability for current and future business needs?
3. Does the solution enable you to manage your certificates' lifecycle?
4. Does the solution provide a certificate management platform?
5. Does the solution issue, install, and automate your certificates to comply with the latest regulations?
6. Does the solution identify, issue, manage, delegate, and automate your certificates' lifecycle (certificate validity) with a single dashboard?
7. Does the solution view, manage, and revoke all certificate types?
8. Does the solution include flexible licensing and subscription options?
9. Does the solution work with industry standards (CA/Browser Forum)?
10. Does the solution support Certificate Authority Authorization (CAA) to enforce an organization's certificate policy?
11. Can the solution provide customized workflows?
12. Is the solution backed by ongoing support and professional services?
13. Does the solution allow the consumption of certificates through free integrations of other tools?

Successfully onboarding a CA

Why choose or switch to Entrust as your dedicated CA?

25+ years

25+ years of experience in Certificate Management with continued investment in PKI use cases

98% renewal rate

98% customer renewal rate

Founding member of the CA Security Council, providing recommended best practices for online security

Founding member of the CA/Browser Forum, working to develop industry standards for TLS/SSL and certificate management

Ranked as one of the fastest-growing CAs globally and a leader in innovation in the latest Frost Rada™ & Sullivan report

Large network of strategic partners including Microsoft, Amazon Web Services Venafi, ServiceNow, Sixscape, Red Sift, and Visa

Offers a single pane of glass to manage public and private digital certificates with a single dashboard, including certificates from other CAs

Entrust Cloud Certificate Services portal can be integrated with Entrust PKI solutions

Subscription-based pricing that scales to ever-changing business needs

Broad solutions portfolio including Certificate Hub, Verified Mark Certificates, eIDAS and PSD2 certificates, PKI as a Service, and Digital Signing as a Service

An innovative and ever-growing CA with certificate-based products and services to manage security and identity use cases covered by public and private PKI technology

Learn more about our digital certificate solutions at entrust.com

Successfully onboarding a CA

Steps to successfully onboarding a CA

Once you've decided it's time to enlist a new or additional CA, there are important steps needed to ensure a successful onboarding experience.

Action	Customer	CA
Set up POC	•	•
Provide domain list (using CT search and discovery)	•	
Provide company name list	•	
Validate domains		•
Validate company names		•
Provide admins and roles list	•	
Validate admins	•	•
Delegate setup	•	•
Inform TLS/SSL subscribers of CA migration	•	
Distribute Intermediate certificates for new CA hierarchy	•	
Maintain list of certificates to be migrated	•	
Establish policies (e.g., certificate expiry notifications, recipients, and escalation procedures)	•	
Create customized certificate request & approval workflow (e-forms)	•	•
Integrate with other third-party software, i.e., Venafi, ServiceNow	•	•
Set up training	•	•

Learn More

Learn more about our digital certificate solutions at entrust.com/resources/certificate-solutions or entrust.com/digital-security/certificate-solutions.
Or contact one of our security experts at entrust.com/contact/sales.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223