Private Dedicated Certification Authority (CA)

A fully managed hosted CA for private trust

Market Challenge

Organizations need a strong chain of trust in order to maintain a secure networking environment. We rely on TLS/SSL certificates to encrypt data for secure server-to-server communication as part of that critical security infrastructure. **>> Learn more**

Solution

The current climate of changing policy for publicly trusted certificates reduces privacy and requires additional administrative effort. Private certificates enable you to bypass the rigor and continual policy changes required for publicly trusted certificates and enable organizations to maintain the privacy of internal infrastructure.

A private dedicated CA gives you full control over TLS/SSL security for server-to-server communications, internal websites, and other applications. It is the easiest method available for establishing policy and gaining visibility into software and infrastructure.

Entrust Certificate Services (ECS), our industry-recognized certificate management platform, makes it even easier to deploy, audit, and manage your complete certificate inventory from a single dashboard.

BENEFITS

- Eliminates the costs of running and maintaining a PKI
- Secure account setup – verifies organization and administrator
- Maintains privacy for internal servers by keeping them off public logs
- Eliminate compliance issues associated with changing policy requirements for public certificates
- Rapid certificate issuance doesn't require validation
- Flexible terms – issue certificates from 10 days to 39 months
- Gain productivity – longer life certificates reduce server touches
- Robust management platform – real-time tracking, alerts, and reporting reduce security lapses
- Consolidated management for both public and private TLS/SSL certificates, including Wildcard
- 24x5 world-class support

Private Dedicated Certification Authority

Private dedicated certification authority at a glance

It's more important than ever for organizations to take a proactive approach to establishing their own security policies. A private dedicated CA is necessary to maintain infrastructure privacy and secure vital communication networks in a cost-effective way.

Eliminate error-prone manual processes and improve productivity with easy-to-manage certificates.

Control your networking environment with flexible naming, SANs, and validity periods for private TLS/SSL certificates minus the public policy that is designed for a different use case.

Secure your internal network communication and keep the presence and naming of internal infrastructure private.

Be proactive about certificate management with full rights to ECS, our robust certificate management platform. You get the information you need when and where you need it.

Features

Full control over internal infrastructure and naming

Maintain privacy

Longer certificate terms (up to 39 months)

No certificate verification

Not subject to public policy

Cloud-based – no system to deploy nor software to manage

Private Dedicated Certification Authority

Certificate Management Features

- Centralized management
- Configurable dashboard
- Auto-installers
- eForms
- Instant issuance
- Reporting and alerts
- Unlimited reissues for TLS/SSL
- Unlimited server licensing
- Flexible subscription plans
- Easy, one-click renewal
- Manage expirations
- Best practices approach

Advantages of a private dedicated CA

Quick setup

Entrust can provide you with a private dedicated CA with a certificate management system exclusive to your organization. A single verification process is needed to prove organization and administrative validation, which follows the same vetting guidelines that are used for OV certificate issuance. Once account-wide verification is complete, you can start issuing private dedicated SSL certificates without further verification.

Differs from a shared private CA

With a shared private CA, the root is shared among a pool of customers, making their use restrictive in some ways. Here are some of the differences that make a private dedicated CA a better choice:

- Full flexibility over server naming – unverified and unlimited domain naming provides full control and flexibility over the naming of your infrastructure.
- More secure - distribute the CA (root) to a limited set and determine who the subscribers will be, giving you absolute control over private trust distribution.

Entrust Private Dedicated CA versus an on-premises PKI

Establishing a private dedicated CA with Entrust brings you greater ease-of-use and cost savings over an on-premises PKI. It is SaaS enabled, simplifying the way you manage certificates while maintaining a secure networking environment.

A private dedicated CA lowers the total cost of ownership per certificate by eliminating the costs of running and managing a PKI infrastructure or OCSP software.

Plus, you get full access to ECS, our robust certificate management platform that streamlines the issuance, tracking, and auditing of your complete certificate population.

Private Dedicated Certification Authority

Differs from a Microsoft CA

Our private dedicated CA is hosted and provides a fully managed experience, delivering certificates without managing a PKI, hardware and software updates, or knowledge retention.

Differs from certificates Issued by a publicly trusted CA

Certificates requiring public trust are subject to policy requirements put forth by industry standard groups and web browsers, which makes sense for certificates used to provide security for a public protocol. However, those requirements are not always ideal for internal security infrastructure and cause additional administrative tasks that are unnecessary for private certificates.

Private dedicated certificates are not subject to:

1. Certificate transparency (CT) logging – All public certificates are required to be CT logged. While the practice makes it easier for organizations to identify rogue certificates, it also brings transparency to internal servers compromising security.
2. Maximum certificate lifetime for public trust – As public certificate lifetime limits decrease, organizations are forced to do more maintenance around certificate renewals. Private certificates can be purchased for up to a 39-month lifetime, reducing administrative tasks.
3. Limitations on the use of non-fully qualified domain names.
4. Validation of the distinguished name (DN) – Customers can put any content in the Organization, Organization Unit, and Locale (C/S/L) fields.
5. Certificate Authority Authorization (CAA) checking – This is another industry standard giving organizations the option to specify which CAs can issue certificates to their organization through their DNS records. CAs are required to check the CAA records prior to certificate issuance.

Use cases for a private dedicated CA

1. Server to server communication.
2. Internal websites that don't require public trust or that have non-fully qualified domain names.
3. Other applications that use non-public TLS/SSL.

Fee schedule

Our package establishes your organization as an issuing CA for private certificates with full rights to the Entrust certificate management platform as part of a monthly subscription plan.

The cost of running a private dedicated CA includes a one-time setup fee, an annual hosting fee, and the cost of the certificates.

Optional annual WebTrust audits are available for an additional fee, if required to help meet your compliance guidelines.

Private Dedicated Certification Authority

TECHNICAL SPECIFICATIONS

The default configuration of a private dedicated CA setup by Entrust

CA Hierarchy

- End-entity certificate products available for issuance from a private dedicated CA offering includes “Private Dedicated TLS/SSL” certificate product.
- Intermediate/Issuing CA provided by default.
- Root CA available as an option Issuing CA.
- Issuing CA is self-signed by default but can optionally be signed by a private dedicated root CA.
- Issuing CA validity – issuing CA can be created with a validity period up to Dec. 31, 2030.
- Issuing CA key size – issuing CAs use RSA 2048 bit keys by default.
- Termination – upon expiration of the agreement, the CA will be terminated.

Optional Root CA Details

- Root CA validity – root CAs are created with a validity period of 20 years for maximum flexibility.
- Root CA key size – root CAs use RSA 4096 bit keys.

Product Details - Entrust “Private Dedicated TLS/SSL” Certificate:

- Permitted key sizes are: RSA 2048, RSA 3072, RSA 4096, and several ECC implementations.
- Revocation checking of end-entity certificates is provided via the standard Entrust OCSP and CRL offering, shared withour public CA infrastructure.
- End entity certificate usage (EKU) support: certificates can be configured to support server authentication, client authentication, or server and client authentication.
- Private dedicated TLS/SSL certificates have no restrictions on domain naming (e.g., subject name and SANs).
- Private dedicated TLS/SSL certificates can be issued for a maximum validity period of 39 months.
- Private trust certificates are NOT logged in the CT logs, both for privacy reasons and because there are no third-party requirements for private trust.
- Private trust certificates are issued without checking Certification Authority Authorization (CAA) records.

Private Dedicated Certification Authority

Frequently asked questions

Am I purchasing a CA infrastructure? If so, can I port the infrastructure from Entrust to my environment at any time?

Entrust is licensing a CA certificate to the customer for the purpose of signing end-entity certificates. Entrust maintains ownership of the private key, issuing and root CA certificates.

Are there any technical constraints on the CA?

Entrust currently offers issuance of private dedicated TLS/SSL certificates from the private dedicated CA offering. Additional certificate types will be made available in response to customer demand.

Does the CA come with a WebTrust audit?

A WebTrust audit is available for the private dedicated CA. Please request it upon placing your order, as it requires an audited CA creation ceremony.

Can I create my own policy for this CA?

Entrust operates all private dedicated CAs in accordance with a common policy, which is based on the high standards set forth by public policy, but with the additional flexibility required for private certificates.

Do my domain names need to be verified by Entrust?

No. Once the initial account setup is complete, there is no additional validation of domain ownership or control.

What certificate types can be issued from a private dedicated CA?

Currently, certificate issuance is available for private TLS/SSL certificates.

Expanded offerings*

Platinum Support is available 24x7.

Discovery+ consolidates management of all certificates by any vendor to our ECS platform.

*Additional fees apply.

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
info@entrust.com entrust.com/contact