Managed Root Certificate Authority (CA)

Many organizations are moving core components of their infrastructure to the cloud to enable cost savings and provide scalability. When running a public key infrastructure (PKI), the challenge is to both secure the root as an offline resource and separately manage the root certificate authority (CA) and issuing sub CAs that need to be accessible online for certificate requests and issuances.

Entrust has the expertise and secure environment necessary to hold the root private key offline and also manage the signing of keys used for online RAs and issuing sub CAs.

If a root CA is compromised, confidence in any of the certificates issued for identification, authorization, and encryption is lost. If someone gains unauthorized access to the root CA, they can issue certificates with arbitrary dates, and you can no longer distinguish between real and fake certificates.

To mitigate the risk of the root CA being accessed by an unauthorized user and ensure the reliability of the CA, it is a best practice to install root CAs offline. This way, the root CA is not connected to a network, and you can keep the CA in a secure area with limited access.

SOLUTION ADVANTAGES

- Fast deployment with low complexity
- No PKI expertise required
- No hardware or software to manage
- Full backup and recovery facility
- Support sub CA infrastructure for multiple Entrust hosted services (PKIaaS and Managed PKI)
- Scales as you grow
- Device-agnostic approach
- Compliance with eIDAS and certified through ETSI and tScheme standards

KEY CAPABILITIES

- Certificate issuance
- Renewal and revocation
- Policy enforcement
- Compliance support
- Reporting and inventory tools
- Lifecycle management for certificates
- Root CA cryptographic keys held in FIPS 140-2 Level 3 HSM
- Annual audited assurance process with customer to validate keys/policy

Learn more about the Entrust Managed Root CA service at entrust.com

Managed Root Certificate Authority (CA)

Entrust Managed Root CA service is a customer-specific PKI root CA designed and built to exacting standards and hosted under a tScheme-approved audit regime as a standalone offline service.

Our root CAs are designed to be the ultimate point of trust in any customer's PKI. This means that you are able to use the root CA as a foundation to build and/or sign one or multiple subordinate issuing CAs, to provide high assurance certificates for your own internal use, or create strong trust with other departments, partners, and suppliers. High assurance of your root CA becomes increasingly important if any part of your PKI infrastructure will be used for third-party trust services or if your CA needs to meet best-practice security standards for accredited systems.

Hosted Root CA

The trust anchor of a PKI is a high assurance root CA. Entrust provides a root CA build and hosting service to its PKI customers.

If you choose to use our root service, your root will be built and hosted securely in an accredited Entrust service center. To give you the highest levels of assurance, our service centers deploy customer roots into the Entrust Certificate Factory, which ensures that the build and operations are controlled and assured to tScheme, ETSI, and ISO 27001 standards.

Following the root CA build, we will undertake a key signing ceremony (KSC) with you, creating the protected key material for the CA and implementing it according to your policy. As this is your PKI, you are the only one who has access to the root CA private keys. These keys are protected by a quorum of HSM control keys of which you hold the majority share. This means that no one can initialize the root to create additional sub CAs or revoke sub CAs without your presence.

After the KSC, Entrust will facilitate root ARL signings as often as required. Signings follow the accreditation and compliance requirements for the specific root CA, according to its policy. We also offer further services related to the root CA, including:

- Sub CA signings
- Root CA and sub CA certificate lifecycle management advice (e.g. hashing algorithms/cryptographic algorithms)
- Policy and certificate profile advice
- Root maintenance
- Root migration/rollover

Learn more about the Entrust Managed Root CA service at entrust.com

Managed Root Certificate Authority (CA)

Security and Assurance

The root CA within our Managed PKI root CA has no external interfaces. It's standalone and offline. The interaction between the root CA and other Entrust PKI managed service components, where applicable, is in an offline process carried out at a frequency agreed upon with the customer. Our security model is based on best practices and ensures a high level of management control.

Secure Your Corporate System Today

Digital certificates allow organizations to leverage encryption and digital signatures to support a variety of security services, including user and device authentication, transaction integrity and verification, and data security.

Entrust Certificate Authority, the world's leading PKI, helps these organizations easily manage their security infrastructure and enables easy management of the digital keys and certificates that secure user and device identities.

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