Entrust Managed Microsoft PKI Service

A cost-effective, secure way to control access to your network, applications, and devices using trusted credentials

HIGHLIGHTS

High assurance, low complexity

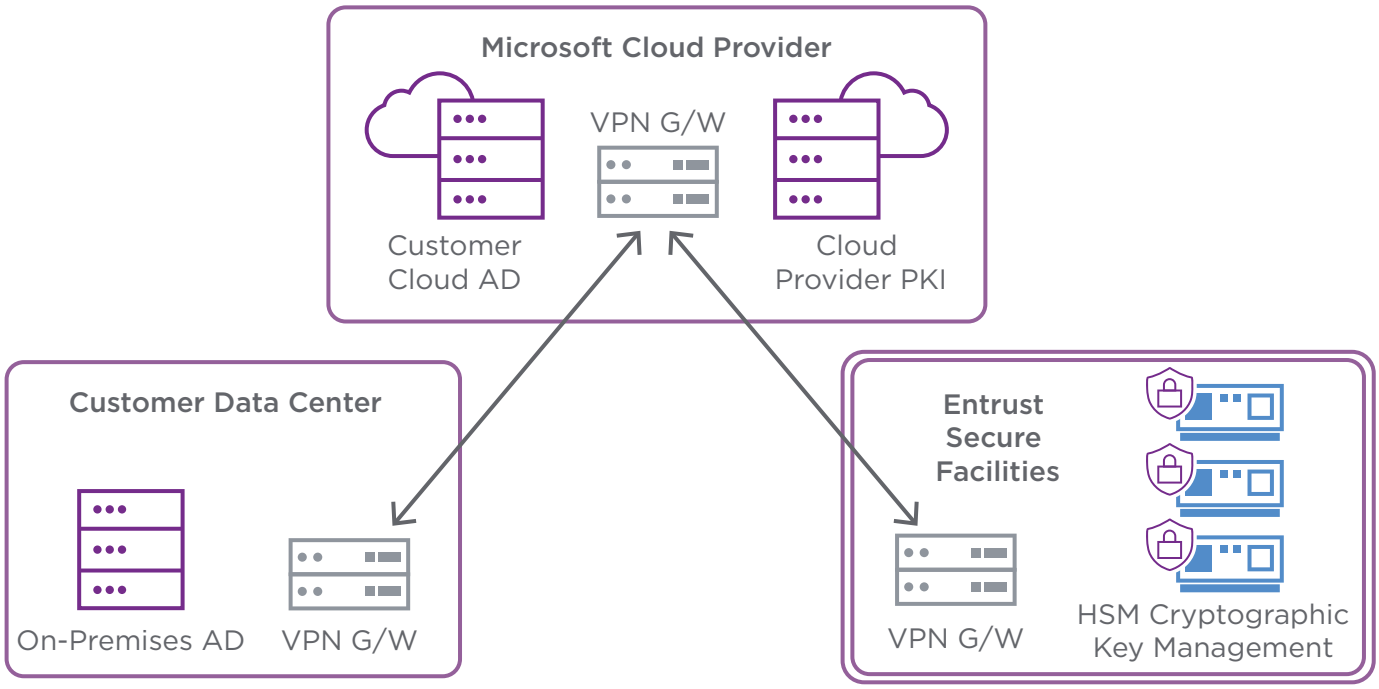
The Entrust Managed Microsoft Public Key Infrastructure (PKI) Service is designed and built to exacting standards. It's low-risk and efficient, and it enables you to retain full control of your PKI without having to worry about the complexities of PKI design, monitoring, and operation. Your own dedicated Microsoft PKI is delivered as a managed service and hosted in your Azure environment.

- Fast deployment with low complexity
- No hardware or software to manage
- No PKI expertise required
- Low start-up and lifetime costs
- Scales as you grow
- Device-agnostic approach
- Built to industry best practices
- Monitored and administered from purpose-built PKI data centers
- Root CA and FIPS 140-2 Level 3 HSMs hosted in certified environments

KEY CAPABILITIES

- Certificate issuance, renewal, and revocation
- Customized policy documentation – CP/CPS
- Intune ready
- Reporting and inventory tools
- Cryptographic keys stored and managed outside of cloud in ultra-secure, audited facilities
- Standalone/offline Root CA managed under your control to high levels of assurance
- Dedicated, customer-specific HSMs or HSM partitions
- Secure integration between on-premises and cloud servers using protected VPN

Managed Microsoft PKI Service



HOW IT WORKS

Your own enterprise PKI in the cloud

Many organizations are moving core components of their infrastructure to the cloud to enable cost savings, improve performance, and provide rapid scalability. It's also possible to put your Microsoft PKI in the cloud, but it's crucial that you maintain sole control of your cryptographic keys. CA keys need to be managed properly under policies and auditable processes, as well as stored in hardware security modules (HSMs). Entrust achieves this by:

- Hosting the offline Root CA and HSMs in our certified data centers
- Giving only your organization access to your Root CA keys

This means you can now have your own two-tier, high assurance enterprise PKI in the cloud with your own dedicated, root and sub CA infrastructure under a Certificate Policy where you are the Policy Authority. This is your PKI, deployed to industry best practices and tailored to your own organization's requirements. The Entrust Managed Microsoft PKI Service will provide you with a solid foundation for your corporate PKI use cases. Entrust will deploy and support your PKI using a fully developed and tested set of procedures and audited processes:

- We do not require admin rights to your Active Directory
- Control over your PKI and its associated business processes remains with you
- For security reasons, the CA keys will be held in FIPS 140-2 Level 3 HSMs hosted in Entrust Secure Data Centers

Managed Microsoft PKI Service

Hosted root CA

The trust anchor of a PKI is a root CA. If you want assurance in your credentials, the root must be highly controlled, kept offline, and operated at equal or higher assurance to your issuing CAs. Entrust provides a root CA build and hosting service. If you choose to use our Root Service, your root will be hosted securely in an accredited Entrust Service Center. To give you the highest levels of assurance, our service centers:

- Are specifically built to host PKI systems
- Can provide assurance processes to WebTrust and ISO 27001 approval, as required

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 cryptographic smart cards, of which you hold the majority share. This means that nobody can initialize the root to create additional sub CAs or revoke sub CAs without your trusted key holder's participation.

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 Certificate 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

Secure your corporate system

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
- Data security

Entrust Security Manager, 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.

Managed Microsoft PKI Service

Learn more at
entrust.com

ENTRUST

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