Cryptography-as-a-Service (CaaS)

Market Challenge: Keeping Control of Your Cryptographic Keys

Cryptographic keys are a critical component for securing IT infrastructure, communications, and applications. While they mathematically offer very strong protection, there's an assumption that the keys are kept secret and access to them is kept secure. This assumption is very difficult to guarantee, as without the proper controls such as policies and audits, systems can easily be compromised.

This problem is exacerbated when IT infrastructure and applications are hosted in the cloud. In these cases, the customer is rarely in control of their own cryptographic keys and cannot guarantee that they won't be compromised.

Management of cryptographic systems and processes is a specialized function. Effective management requires in-depth knowledge of IT security equipment such as HSMs and processes, procedures, and audit requirements specific to cryptography. Furthermore, even with the specialist skills to comply with your security policies, the hosting provider may still control the cryptographic key material, giving them unrestricted access to sensitive data and/or cryptographic signing processes, which poses a very high security risk.

BENEFITS

- Fast deployment with low complexity
- No hardware or software to manage
- No HSM expertise required
- Low startup and lifetime costs
- Highly available, resilient architecture
- High performance via load balancing and fast processing
- Shared or dedicated secure backup of key material
- Suitable for any key type (e.g., signing, encryption)
- 99.5 percent availability

Learn more about Entrust Cryptography-as-a-Service at entrust.com

Cryptography-as-a-Service (CaaS)

The Solution

Entrust specializes in providing cryptographic services to government and commercial organizations. Our Cryptography-as-a-Service (CaaS) solution uses off-the-shelf HSMs that are certified to FIPS 140-2 Level 3, EAL4+ validated and configured in a high availability cluster to provide resilient cryptographic processing power, as needed.

CaaS supports standard cryptographic calls to HSMs from application and storage programs or infrastructure components that utilize a cryptographic interface. The key management procedures and policies are delivered by cryptographic expert operators according to best practices.

CaaS ensures that a cloud or third-party service provider doesn't have access to the key material, even when key material needs to be revoked or updated for key rollover. Key management processes are performed by security cleared staff within the Entrust facility under ISO 27001 certified defense-in-depth security controls.

Your dedicated partitions on our HSM clusters are connected to your applications by VPN or other secure connections. The HSMs are then managed under strict policy controls. Backup of your key material can be hosted either by Entrust or at your own data centers.

Cryptography-as-a-Service (CaaS) at a glance

Cryptography-as-a-Service (CaaS) is an efficient, cost-effective way to protect your data and systems in the cloud while giving you complete control over your keys. It enables you to use certified, high-performance hardware security modules (HSMs) without employing crypto experts or buying expensive hardware and having unused capacity. CaaS also allows you to maintain master control of customer cryptographic keys.

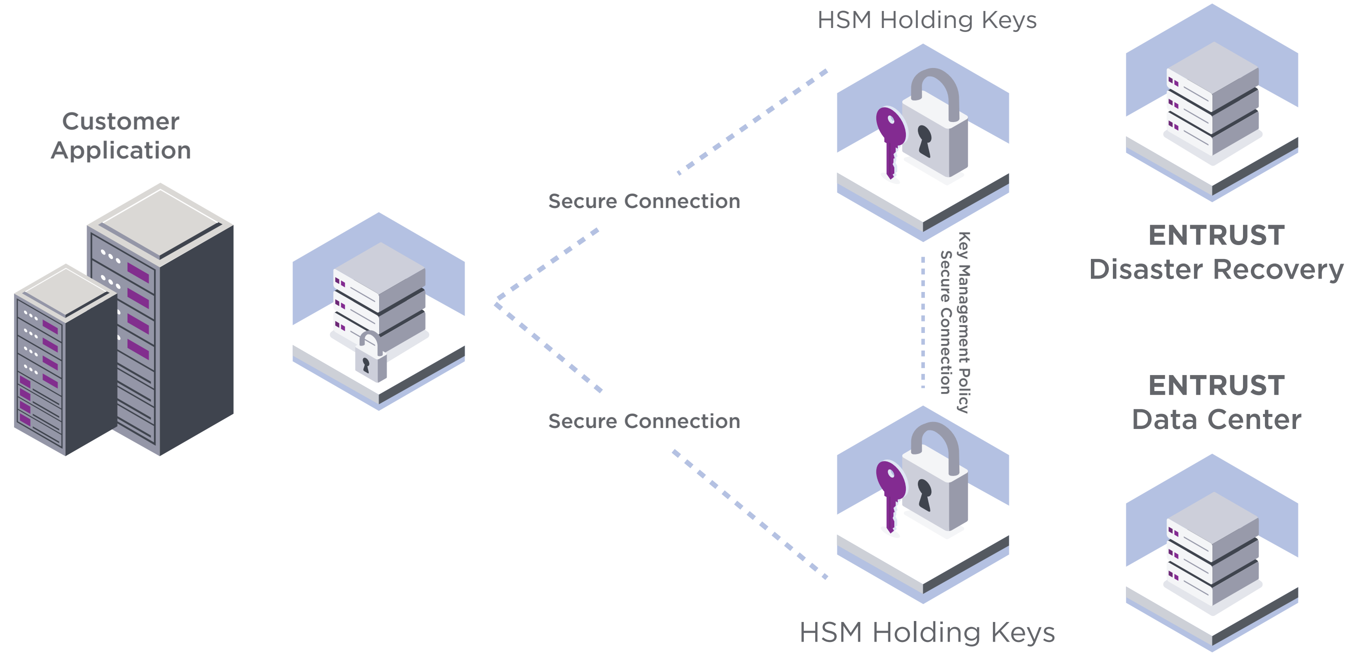
CaaS allows an organization to consume cryptographic processing from the Entrust secure data center of your choice to provide HSM services for your in-house or cloud-based applications and data. It enables multiple customer systems to use as much or as little cryptographic processing as required.

Key Capabilities

- Keys are always stored in FIPS 140-2 Level 3 certified and EAL4+ validated hardware
- Supports all the major algorithms and cryptographic APIs
- Cryptographic keys stored/managed in secure facilities
- Secure partitioning of key material for multiple requirements
- Two-person control of sensitive cryptographic operations

Learn more about Entrust Cryptography-as-a-Service at entrust.com

Cryptography-as-a-Service (CaaS)



HOW IT WORKS

High availability

Entrust high-performing and lightning-fast HSMs are set up in a high-availability (active-active) architecture. The HSMs load balance with failover between local units and sites for redundancy, allowing us to deliver 99.5 percent availability, aligned with the SLAs of the cloud hosting providers.

Backup and restore

Encrypted key material is backed up onto a separate HSM backup device, providing defense in depth and a keys-in-hardware strategy, which delivers the strongest levels of key protection for application keys.

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 Security Manager, a world-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