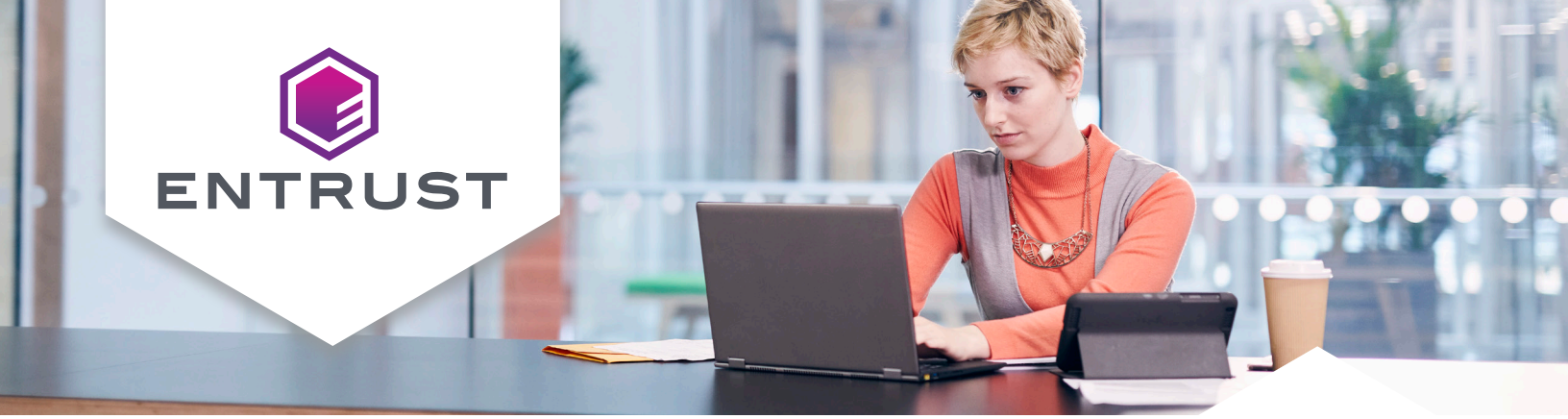


Entrust Double Key Encryption for Microsoft Azure Information Protection

HIGHLIGHTS

Extend control and security over sensitive data in hybrid and cloud environments

- Apply two layers of security to your most sensitive content in Azure cloud
- Encrypt so even Microsoft does not have ability to access your content
- Own and fully control your key and the software that generates your key
- Host your key and store your critical data in the location of your choice
- Manage user access to your key and the content protected by the key

KEY FEATURES & BENEFITS

Entrust Double Key Encryption for Microsoft Azure Information Protection (AIP), offered by Entrust Professional Services, is designed to help enterprises protect their most sensitive content in Microsoft 365.

- Integrates with certified Entrust nShield® HSMs to provide a root of trust for the protection of sensitive customer keys.
- The tools and hardware give enterprises complete ownership and control of the software that underpins the double key generation process, with no Microsoft footprint on the customers' premises.

Double Key Encryption enables organizations to use hybrid-computing environments with added levels of protection, control, and assurance. As part of the Microsoft AIP offer, the solution enables enterprise customers to select who has permissions to access associated keys and decrypt content. Enterprises can store encrypted data on-premises or in the cloud, remaining unreadable to Microsoft.

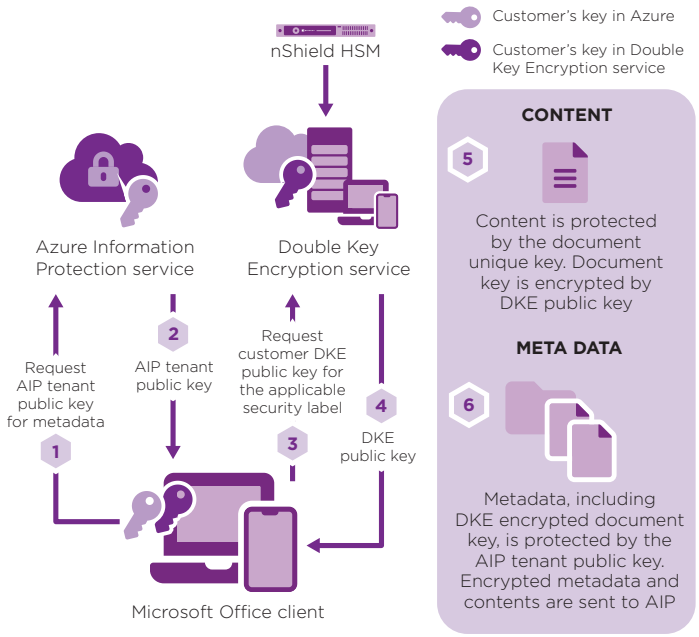
Replacing Microsoft Hold your Own Key (HYOK), Double Key Encryption does not require enterprise customers to operate their own Active Directory and Rights Management servers. Instead, customers are empowered to provide their own cryptographic keys in real time.

Double Key Encryption for Microsoft Azure

HOW IT WORKS

Double Key Encryption utilizes two component cryptographic keys to protect highly sensitive data across the enterprise – a Microsoft key and a customer key.

- Document content is locally encrypted within the client application, using a unique random AES key per document.
- The unique document key is encrypted using the DKE customer key for the specific security label. The DKE private key is protected using nShield HSMs on-premises
- The Microsoft key is used to encrypt the document metadata.
- The process prevents Microsoft from having access to the key and the customer content in Azure.

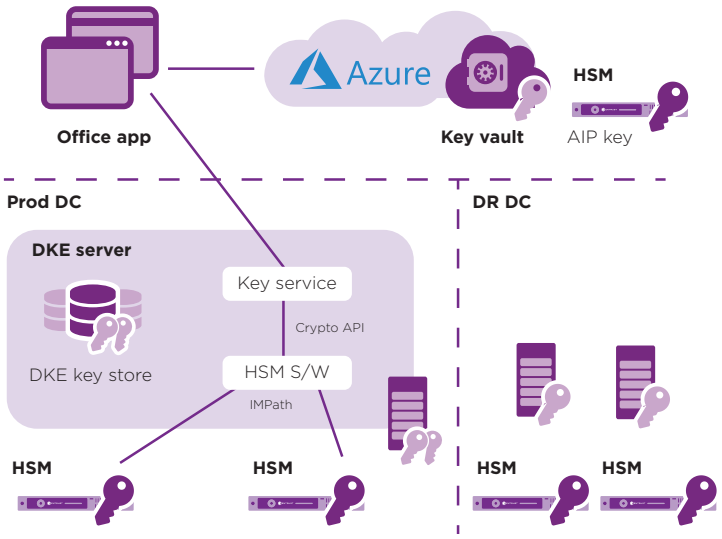


TECHNICAL SPECIFICATIONS

Integrating Entrust nShield HSMs

Entrust nShield HSMs hold the master key that protects the Double Key Encryption server and key store. Four nShield HSMs are typically deployed for redundancy across production and disaster recovery environments.

Entrust Double Key Encryption is supported by FIPS 140-2 Level 3 and Common Criteria EAL4+ certified nShield Solo XC (PCIe) and nShield Connect XC (network-attached) HSMs.



Double Key Encryption for Microsoft Azure

Getting started

To use Entrust Double Key Encryption for Microsoft AIP, you will need:

- Entrust Double Key Encryption solution
- Entrust nShield Solo or nShield Connect HSMs

Entrust HSMs

Entrust nShield HSMs are among the highest-performing, most secure and easy-to-integrate HSM solutions available, facilitating regulatory compliance and delivering the highest levels of data and application security for enterprise, financial, and government organizations. Our unique Security World key management architecture provides strong, granular controls over access and usage of keys.

Learn more

To find out more about Entrust nShield HSMs, visit **entrust.com/HSM.** To learn more about Entrust's digital security solutions for identities, access, communications, and data, visit **entrust.com.**

To find out more about Entrust nShield HSMs:

HSMinfo@entrust.com

entrust.com/HSM

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

HS22Q1-v2-hsm-entrust-double-key-encryption-azure-information-protection-ds

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