Published February 13, 2018

EXECUTIVE SUMMARY

- Encryption can help with data security and data privacy by providing an added layer of defense in depth to protect customer data, but keep in mind that SaaS features require the ability to reason, or compute, against the customer's data.
- Microsoft uses some of the strongest encryption protocols in the industry to provide a barrier against unauthorized access to customer data.
- With Office 365, customer data is encrypted both in transit and at rest by default with no additional licenses or action.
- Native encryption features offered Office 365 can be added for increased protection.
- Office 365 offers flexible encryption key management options to further help organizations meet their compliance needs as they move to the cloud.
- There are a variety of risks that can be reduced by encryption for Office 365, but good data protections strategies include other capabilities that can be used with encryption.

Table of Contents

0. Introduction **3**

1. Why use encryption **3**

How encryption works 3

Why use encryption 3

Key Principle of SaaS Encryption 4

2. Encryption for Office 365 ..... **4**

Your Office 365 data encrypted by default 4

Additional encryption options 4

3. Encryption Key Options for Office 365 ..... **5**

Cloud First Customers – Microsoft Managed Keys 5

Compliance Focused Customers – Customer Managed Keys (in Azure Key Vault) 5

Compliance First Customers – Customer Managed Keys (On-Premises/Hybrid) 7

5. Risks reduced by Encryption for Office 365 ..... **8**

6. Other data protection capabilities in Office 365 ..... **9**

7. Resources **10**

0. Introduction

The era of digital transformation is here. Business leaders are busy rethinking how they can use technology to drive new customer value and revenue. Driven by a sense of urgency to digitally transform the workplace, organizations of all sizes—and across all industries—feel the pressure to embrace digital change. However, change is hard.

As data grows exponentially, managing the risks and complexity of data is challenging: not only must organizations protect their data from growing threats, but they must also maintain compliance with various regulatory, industry and internal requirements related to data security and data privacy.

Encryption is extensively considered to be one method that can be used as part of a broader data protection strategy. When customers use the Microsoft's enterprise cloud service, their data is protected by a variety of technologies and processes, and various forms of encryption.

When organizations use Office 365, they can expect customer data to be encrypted both in transit and at rest by default. Additional encryption capabilities can be added for increased protection. And for customers who have data security or privacy requirements that are driven by compliance, Office 365 offers flexible encryption key management options to further help organizations meet their compliance needs as they move to the cloud.

To help customers that are beginning their journey on encryption, in this document you will find a high-level view of the encryption capabilities offered in Office 365, and what concerns and risks to customer data each capability may help mitigate. It's not meant to be comprehensive, but it will introduce what encryption can do to protect and control data. For a deeper view on how the encryption capabilities are implemented and managed, we recommend the additional reading material at the end of the document under resources.

This document and the information reflects what we offer from the date it was published.

1. Why use encryption

How encryption works

Encryption is the process of encoding messages or information in such a way that only authorized parties can read it protect against data theft or failures in physical security, as well as against eavesdropping of data in transit.

Most encryption methods use one or more keys. Those keys are what can unlock the ability for an authorized party to read the data that's been made unintelligible. Keys can be used to encrypt data, decrypt data, or both. When a key is the means of decrypting data, the ability to use that key means that you are an authorized party – you can read the data.

Why use encryption

There are several benefits to using encryption as one component to your broader data protection strategy. Encryption can help with data security and data privacy by providing an added layer of defense in depth to protect customer data. Encrypting information renders it unreadable to unauthorized persons, even if they break through firewalls, infiltrate a network, get physical access to devices, or bypass the permission on local machine. Encryption can help protect against data theft or failures in physical security, as well as against eavesdropping of data in transit. For example, if a malicious attacker

got a hold of encrypted data, and is not authorized to use the key that can decrypt the data, the data would be useless. Encryption is also commonly brought into compliance discussions as it can help meet regulations or internal requirements that look to control or protect the confidentiality of certain data.

For example, the financial services industry is subject to some of the most stringent and complex regulations, stemming from lessons learned from financial failures over the past 10 years. The industry is regulated for anti-money laundering, fraud protection, customer data protection, and much more with regulations such as MiFID, SEPA, ISAE3402, and industry standards like PCI-DSS.

Key Principle of SaaS Encryption

As you learn about the different encryption capabilities, it's important to understand a key principle regarding SaaS and the use of encryption today. SaaS features require the ability to reason, or compute, against the customer's data. A very simple example of this is a rule in a cloud email service that instructs the service to send a copy of any email containing the keyword "legal" to a mailbox for legal hold reasons. Clearly, if the body of the email is encrypted and the email service cannot use the encryption key to decrypt the contents, it cannot perform this simple computation. It's crucial to point out that SaaS is, by nature, is a software application and software applications provide computational features. So, using encryption with the intent of making the data unreadable by the cloud service blocks the innovative features that are presumably the purpose of purchasing SaaS.

2. Encryption for Office 365

Customer data within Microsoft's enterprise cloud service is protected by a variety of technologies and processes, including various forms of encryption. Microsoft uses some of the strongest encryption protocols in the industry to provide a barrier against unauthorized access to customer data. Proper key management is an essential element in encryption best practices, and Microsoft helps ensure that encryption keys are properly secured.

Office 365 provides multiple encryption capabilities that protect customer data without impacting the value-added services that many customers come to the cloud for. Read further to learn about what the encryption offerings provided in Office 365.

Your Office 365 data encrypted by default

Customers can feel confident that their Office 365 data is encrypted both at rest and in transit by default.

For data in transit, Office 365 uses industry standard secure transport protocols, such as Transport Layer Security between our customers clients/devices and Microsoft datacenters. All customer facing servers negotiate using TLS by default with client machines to secure the customer data.

For data at rest, Office 365 uses various technologies. Office 365 servers use BitLocker to encrypt the disk drives containing customer data at rest at the volume-level. In addition to volume-level encryption, Office 365 uses service encryption to encrypt at the application level. Service encryption provides more granular layer of encryption for mailboxes and files in Office 365.

Additional customer-managed encryption options

Additional customer managed encryption options are available to provide granular layer of protection at the content level.

Office 365 Message Encryption

For emails, Office 365 Message Encryption is an easy to set up email service that allows you to send encrypted and rights protected mails to anyone. Admins can apply automatic policies through transport rules that encrypt mail if it matches certain criteria. Users are can also easily apply protection through Outlook (web, desktop) and share protected messages sent inside or outside the organization. Office 365 Message Encryption leverages the protection feature in Azure Information Protection without additional licenses outside of the core Office 365 E3 or E5 offering.

Azure Information Protection for Office 365

The protection feature in Azure Information Protection uses encryption, identity, and authorization policies that stay with the protected document and email to help you be in control of your data, even when it is shared with other people. Customers can also use Azure Information Protection to help classify and label documents and emails to further manage and control data –the labels can be used to classify and apply protection, and once classified you can track and control how it is used. More information on this can be found here.

3. Encryption Key Options for Office 365

Meeting compliance obligations are important to any organization. There are some customers who have compliance requirements that call out certain key arrangements with their cloud service provider. For these customers we provide several encryption key management options to meet their business needs.

Cloud First Customers – Microsoft Managed Keys

Microsoft managed keys are when the tenant private key(s) are stored and managed by the service (Microsoft). Cloud first customers that do not have stringent compliance needs, leveraging Microsoft managed keys as the ideal option.

Microsoft Managed Keys are simple to manage, do not require encryption expertise, and provided with no additional subscriptions or configurations. This is option readily available by default with every tenant that uses Office 365.

Compliance Focused Customers – Customer Managed Keys (in Azure Key Vault)

For some customers, Microsoft Managed Keys may not be meet their compliance obligations. Certain compliance requirements may be driving overall security needs – such as where the keys can go, how the keys are managed and who can operate on the keys. For example, in some regions customers have regulatory obligations that state they need to have certain key arrangements with their cloud service provider. Even more common, certain large organizations have HSM software, hardware and other processes in place to manage their keys – therefore they may be looking to extend this into the cloud. For these customers, customer managed keys are offered in Office 365.

Customer Managed keys are when the customer imports or generates keys in the Hardware Security Module (HSM) in Azure Key Vault – and manages and controls the keys from Azure Key Vault. The customers' root keys never leave the HSM boundary.

Office 365 provides customers the option to provide and control their keys in Azure Key Vault, for their Office 365 data at-rest with Customer Key, and for their Office 365 data in-transit with Bring Your Own Key in Azure Information Protection.

With these customer managed key options in Office 365, organizations continue to receive a seamless experience in Office 365, and the value-added services such as anti-spam/malware, data loss prevention, eDiscovery, archiving ect., continue to work.

Customer Key in Office 365

Customer Key enhances the ability for organizations to meet the demands of organizations that have compliance requirements that specify key arrangements with the cloud service provider. With Customer Key, organizations can provide and control their encryption keys for their Office 365 data at-rest at the application level. As a result, customers may exercise their control and revoke their keys, should they decide to exit the service. By revoking the keys, the data is unreadable to the service and will put the customer on path towards data deletion. Lastly, managing and protecting keys is crucial but can be difficult. Customer Key includes an availability key to protect against data loss. The availability key is a root key that is provisioned and protected by Microsoft and is functionally equivalent to the root keys that are supplied by the customer for use with Customer Key. The availability key provides a strong key escrow model which reduces the risk of all the keys being unintentionally lost or destroyed. Additionally, to meet our rigorous SLA for service uptime, the availability key is also used for service availability. Although in our experience service failures are rare, due to transient AAD or network issues, not being able to access Office 365 content can be problematic; therefore, if the service cannot reach the customer's root keys in Azure Key Vault and we do not receive a response that indicates the customer has intended to block access to their root keys, we will fall back to the availability key to complete the operation. The availability key is unique to Customer Key and should the customer decide to exit the service, the availability key is purged as part of the data deletion process.

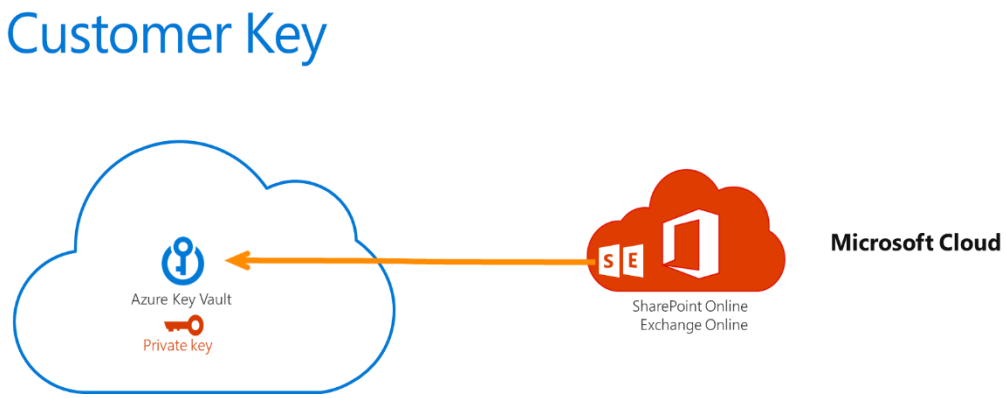

DIAGRAM - Here is a simplified view of customer managed keys managed in Azure Key Vault. The customer provides and manages their asymmetric private keys in Azure Key Vault. The customers' private keys do no not leave Azure Key Vault's HSM boundary and customers have the control to revoke their private keys to make the data inaccessible to the service, and initiate the path towards data deletion.

Bring Your Own Key (BYOK) in Azure Information Protection

With Bring Your Own Key (BYOK) in Azure Information Protection, customers may provide and control their own encryption keys for their Office 365 data in-transit at the content level. For example, for Office 365 Message Encryption, customers may provide and control their own encryption keys for their sensitive emails. Office 365 Message Encryption leverages the protection features in Azure Information Protection,

therefore Azure Information protection handles key management and interfacing with Azure Key Vault. Azure Key Vault performs the encryption operations and the customers private root keys remain protected in the HSM boundary.

Compliance First Customers – Customer Managed Keys (On-Premises/Hybrid)

For a very small subset of highly-regulated organizations that have compliance obligations requiring them to have physical access and possession of their private keys so that their very most sensitive data is inaccessible to the Microsoft Cloud Service—Microsoft supports Hold Your Own Key (HYOK) with Azure Information Protection and S/MIME.

Hold Your Own Key (HYOK) with Azure Information Protection

HYOK is an isolated on-premises Azure Directory rights Management Service (AD RMS) instance that provides a different private key to secure this data. Because the key is stored and managed in an on-premises environment, it protects data that remains on-premises and away from all cloud instances. If shared outside of this the data would be opaque to unauthorized parties including the cloud service provider.

HYOK is not for everyone, and it is certainly not intended for every piece of data. HYOK is a special tool, for a special purpose: data opacity at all costs. Generally, we recommend this to be applied to less than one percent of data. While Office 365 does support HYOK with Azure Information Protection, Office 365 services will be significantly limited with this configuration. Because the data that is protected will be opaque to the cloud, many of the most powerful Office 365 experiences will be unavailable: no anti-malware/spam, Delve, eDiscovery, search, and so forth. Any transport rules and DLP policies will not be able to look at this data, and any anti-virus services or DLP will need an entirely different environment.

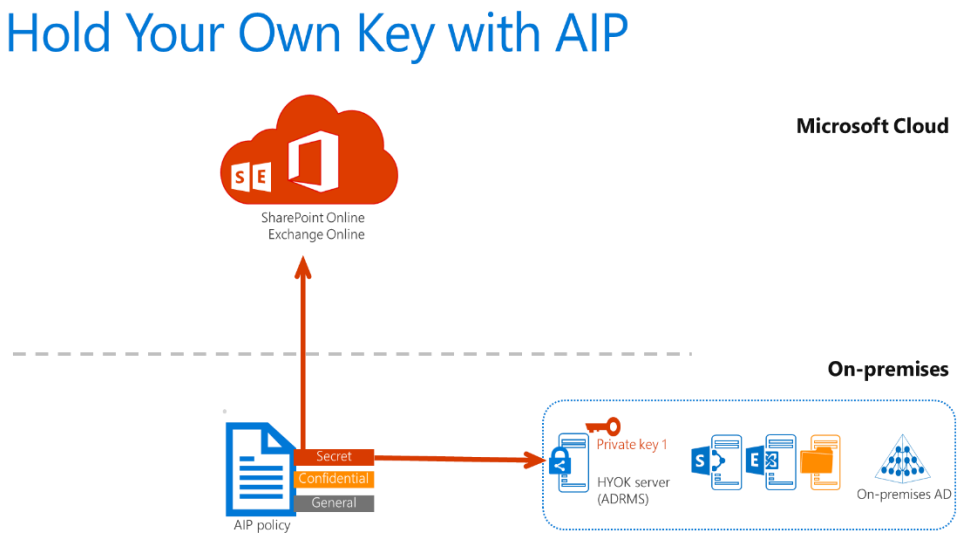

DIAGRAM - Here is an example of an HYOK topology. Customer has on-premises AD, AD RMS server and HSM. Customer's private keys are managed in the on-premises HSM, and used by the on-premises AD RMS server. The customer physically possesses their private keys and does not share these keys with the Microsoft cloud. The AIP classification labels are bound to the Azure RMS server – so when an end user applies the specific label, which in this example is 'Secret' it will be protected with HYOK.

S/MIME

Office 365 also supports S/MIME. S/MIME is a certificate-based encryption solution that allows you to both encrypt and digitally sign a message. The public certificates are distributed to an organization's on-premises Active Directory and stored in attributes that cannot be replicated to an Office 365 tenant. The private keys remain on-premises and are never transmitted to Office 365. Therefore, Office 365 services that need to read and reason over the data will not work.

5. Risks reduced by Encryption for Office 365

There are a variety of risks that can be reduced by encryption for Office 365. Encryption can help reduce the risk of data compromise from an attack by a malicious outsider or from an accidental data leak by one of your users. Encryption can also help reduce the risk of non-compliance from regulations that look to protect sensitive personal information, or various internal compliance obligations such as customer contractual agreements or internal security policies, that drive the customers' overall security decisions.

See below a high-level table and review the definitions to better understand how each encryption technology can help reduce various risks to customer data.

Risk Area		TLS	BitLocker	Service Encryption	Office 365 Message Encryption	Customer Key	BYOK with AIP	HYOK with AIP	S/MIME
Attack from malicious outsider		x	x	x	x	x	x	x	x
Accidental leak of data (user)					x		x	x	x
Non-Compliance (Regulatory/ Internal)		x	x	x	x	x	x	x	x
Offered In		All commercial Office 365 SKUs	All commercial Office 365 SKUs	All commercial Office 365 SKUs	Office 365 E3/E5*	Office 365 E5** + Azure Key Vault Subscription	Office 365 E3/E5* + Azure Key Vault Subscription	EMS E5 or AIP Plan P2 Add-On	N/A

*Also offered as add-on for full list go here.

**Also offered as add-on to Office 365 E3 with Advanced Compliance SKU.

Definitions

TLS:

Reduces risk of data compromise due to snooping or man-in-the-middle attacks if information is intercepted as it travels over the network. TLS doesn't encrypt the message, just the connection. If your recipient's mail servers are not does support TLS encryption, then the message will be sent unencrypted. We suggest customers adding Office 365 Message Encryption to their sensitive emails in this scenario.

BitLocker:

Reduces the risk of data compromise due to lapses in processes or controls (such as access control or hardware recycling processes) that enable someone to gain physical access to disks containing sensitive data.

Service Encryption:

Reduces risk of data compromise due to an attack by a malicious outsider. The data cannot be decrypted without access to keys. Service encryption also provides a granular layer of protection at the application layer on top of BitLocker for customers' Office 365 data at-rest.

Service Encryption with Customer Key:

In addition to benefits of service encryption above, Customer Key can help reduce the risk of non-compliance due to obligations surrounding how or where the customers' encryption keys are controlled or managed —or obligations related to having the explicit control to delete data when exiting the service.

Office 365 Message Encryption:

Reduces the risk of data compromise due to an attack by a malicious outsider, or due to an accidental data leak by an employee. The new Office 365 Message Encryption includes the protection feature in Azure Information Protection to encrypt and rights protect emails. When the new Office 365 Message Encryption is applied to emails, the email is not only protected throughout the lifecycle of the email but also provides an added layer of encryption on top of default encryption capabilities offered in Office 365 (TLS, BitLocker, Service Encryption).

BYOK with Azure Information Protection for Office 365 Message Encryption:

In addition to benefits of Office 365 Message Encryption, BYOK with Azure Information protection can help reduce the risk of non-compliance due to obligations surrounding how or where the customers' encryption keys are controlled or managed.

HYOK with Azure Information Protection:

Key is stored and managed in an on-premises environment, it protects any data that remains on-premises and away from all cloud instances. If shared outside of this the data would be opaque to unauthorized parties including the cloud service provider.

S/MIME:

S/MIME ensures that the email encrypted by S/MIME can only be decrypted by the direct recipient of the email. The cloud service provider and unauthorized users cannot see the contents of the email. Office 365 supports S/MIME; however, Office 365 services are significantly limited on data that is encrypted with S/MIME.

6. Other data protection capabilities in Office 365

Encryption can be useful a technology to help customers meet their compliance and data protection needs; however, it should not be used in isolation. We recommend customers consider additional data protection capabilities to complement the encryption solutions offered in Office 365. Here are just a few to consider:

Data Governance

The benefits of implementing a comprehensive data governance strategy are two-fold, reduced cost of storing data and perhaps more importantly reduced risk of keeping data that is no longer relevant but still

needs to be protected. With the data governance capabilities Office 365 customers are able to use intelligence to classify, protect and retain data in their environment, and defensibly dispose of data that is redundant, obsolete or trivial.

Data Loss Prevention

Customers may leverage Office 365 Data Loss Prevention (DLP) to identify, monitor and protect sensitive information in your organization through content scanning. Not only will DLP detect sensitive information types such as credit card numbers or national identity numbers, customers can apply protections such as blocking access, showing policy notifications or encryption emails using Exchange Transport Rules.

Access Control

While there is no standing access to customer data, which is controlled by our access control system, for added control, with Customer Lockbox customers can be added to the workflow before access is provided to the Microsoft service engineer during service operations.

7. Additional resources

For customers doing a risk assessment, we recommend reading a deeper encryption whitepaper offered at https://aka.ms/mcsce. This looks across our encryption capabilities in the Microsoft Cloud.

For all else please refer to the resources below.

Encryption

- Microsoft Cloud Encryption Whitepaper
- Common misconceptions and truths of SaaS encryption

Customer Key in Office 365

1. Customer Key Set Up
2. Customer Key Blog
3. Customer Key FAQ
4. Customer Key Webinars
    - Deep Dive on Customer Key

Office 365 Message Encryption

1. Office 365 Message Encryption Blog
2. Setting up Office 365 Message Encryption
3. Office 365 Message Encryption Webinars
    - Protect and control your sensitive emails

BYOK and HYOK with AIP

1. Encryption key management strategies for compliance (for Azure Information Protection)
2. Hold Your Own Key with Azure Information Protection Blog
3. Hold your own key (HYOK) requirements and restrictions for AD RMS protection

Access Control

Customer Lockbox

1. Customer Lockbox 2 Min Video

2. Office 365 - Customer Lockbox SOC 1 SSAE 16 Type I Report
3. Customer Lockbox Webinar
    - Own your data with next generation access control technology in Office 365

Terms & Conditions