Content Encryption in Microsoft Office 365

Published: January 23, 2017

This document provides an overview of the various encryption technologies that are currently available or recently announced for Office 365, including features deployed and managed by Microsoft and by customers

Contents

Introduction

Customer content within Microsoft Office 365 is protected by a variety of technologies and processes, including various forms of encryption. Microsoft uses service-side technologies in Office 365 that encrypt customer content[1] at rest and in-transit. For content at rest, Office 365 uses volume-level and file-level encryption. For content in-transit, Office 365 uses multiple encryption technologies, such as Transport Layer Security (TLS) and Internet Protocol Security (IPsec). Office 365 also includes additional encryption options that are customer-managed, but irrespective of customer configuration, customer content stored within Office 365 is protected. Validation of our crypto policy and its enforcement is independently verified through the multiple third-party auditors.

In accordance with the Public Key Infrastructure Operational Security Standard, which is a component of Microsoft Security Policy, Office 365 leverages the cryptographic capabilities that are directly a part of the Windows Operating System for certificates and authentication mechanisms (e.g. Kerberos). Office 365's FIPS 140-2 cryptographic modules used for transmitted information are certified by the National Institute of Standards and Technology (NIST). Relevant NIST certificate numbers for Microsoft can be found at http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm. Any time cryptographic capabilities are employed to protect the confidentiality, integrity, or availability of data within Office 365, the modules and ciphers used are FIPS 140-2 validated.

Encryption of Customer Content at Rest

Encryption of Office 365 customer content at rest is provided by multiple service-side technologies: BitLocker volume-level encryption for Office 365 servers, and file-level encryption in Skype for Business, OneDrive for Business and SharePoint Online. In addition, Microsoft is adding capabilities to Exchange Online known as Mailbox-Level Encryption.

Volume-level Encryption

Office 365 servers use BitLocker to encrypt the disk drives containing log files and customer content at rest at the volume-level. BitLocker encryption is a data protection feature that is built into Windows. BitLocker is one of the technologies used to safeguard against threats in case there are lapses in other processes or controls (e.g., access control or recycling of hardware) that could lead to someone gaining physical access to disks containing customer content. In this case, BitLocker eliminates the potential for data theft or exposure because of lost, stolen, or inappropriately decommissioned computers and disks.

BitLocker is deployed with Advanced Encryption Standard (AES) 256-bit encryption on disks containing customer content in Exchange Online, SharePoint Online, and Skype for Business. Disk sectors are encrypted with a Full Volume Encryption Key (FVEK), which is always encrypted with the Volume Master Key (VMK), which, in turn, is bound to the Trusted Platform Module (TPM) in the server. The VMK directly protects the FVEK and therefore, protecting the VMK becomes critical. The

[1] Exchange Online mailbox content (e-mail body, calendar entries, and the content of e-mail attachments), SharePoint Online site content and the files stored within sites, and files uploaded to OneDrive for Business.

following figure illustrates an example of the BitLocker key protection chain for a given server (in this case, an Exchange Online server).

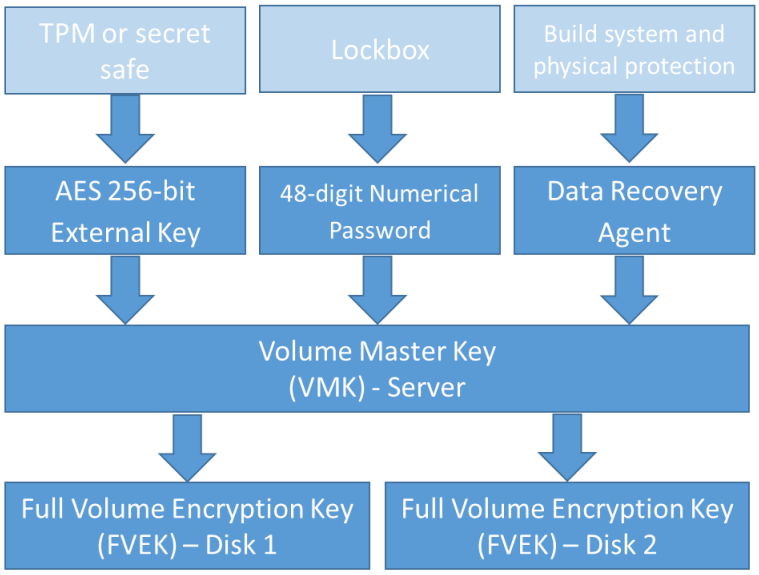

Figure 1 - BitLocker Protection Chain for Exchange Online servers

The following table describes the BitLocker key protection chain for a given server (in this case, an Exchange Online server).

KEY PROTECTOR	GRANULARITY	HOW GENERATED?	WHERE IS IT STORED?	PROTECTION
AES 256-bit External Key	Per Server	BitLocker APIs	TPM or Secret Safe	Lockbox / Access Control
			Mailbox Server Registry	TPM encrypted
48-digit Numerical Password	Per Disk	BitLocker APIs	Active Directory	Lockbox / Access Control
X509 Certificate as Data Recovery Agent (DRA) also called Public Key Protector	Environment (e.g., Exchange Online multitenant)	Microsoft CA	Build System	No one user has the full password to this certificate. The password is under physical protection.

Table 1 – BitLocker Protection Chain for Exchange Online Servers

BitLocker key management involves the management of recovery keys that are used to unlock/recover encrypted disks in an Office 365 datacenter. Office 365 stores the master keys in a secured share, only accessible by individuals who have been screened and approved. The credentials for the keys are stored in a secured repository for access control data (what we call a "secret store"), which requires a high level of elevation and management approvals to access using a just-in-time access elevation tool. All elevated access is both approved and logged by a group other than the group requesting access.

BitLocker supports keys which generally fall into two management categories:

- BitLocker-managed keys, which are generally short-lived and tied to the lifetime of an operating system instance installed on a server or a given encrypted disk. These keys are deleted and reset during server reinstallation or disk formatting.
- BitLocker recovery keys, which are managed outside of BitLocker but used for disk decryption. BitLocker uses recovery keys for the scenario in which an operating system is reinstalled, and encrypted data disks already exist. Recovery keys are also used by Managed Availability monitoring probes for BitLocker in Exchange Online where a responder may need to unlock a disk.

BitLocker-protected volumes are encrypted with a full volume encryption key, which in turn is encrypted with a volume master key. BitLocker uses Federal Information Processing Standards (FIPS)-compliant algorithms to ensure that encryption keys are never stored or sent over the wire in the clear.[2] The following list of requirements have been validated for BitLocker:

- Cryptographic Module Specification (Section 2 of Spec)
- Cryptographic Module Ports and Interfaces (Section 2 & 4 of Spec)
- Finite State Model
- Operational Environment (Section 6.1.2, Item 3 & 4)
- Design Assurance
- Mitigation of Other Attacks
- Self-Tests (Section 8)

Because the Office 365 implementation of customer content-at-rest-protection does not deviate from the default BitLocker implementation, the deployment of BitLocker in Office 365 is FIPS 140 Level 2-validated, and meets these requirements by default.

File-Level Encryption

In addition to using volume-level encryption, Skype for Business, SharePoint Online, and OneDrive for Business also use file-level encryption.

Skype for Business

In Skype for Business, customer content at rest may be stored in the form of files or presentations that have been uploaded by meeting participants. The Web Conferencing server encrypts content using AES with a 256-bit key. The encrypted content is stored on a file share. Each piece of content is encrypted using a different randomly generated 256-bit key. When a piece of content is shared in a conference, the Web Conferencing server instructs the conferencing clients to download the encrypted content via HTTPS. It sends the corresponding key to clients so that the content can be decrypted. The Web Conferencing server also authenticates conferencing clients before it allows the clients access to conference content. When joining a Web conference, each conferencing client establishes a SIP dialog with the conferencing focus component running inside the front-end server over TLS first. The conferencing focus passes to the conference client an authentication cookie

[2] To be to FIPS 140-2 compliant, a cryptographic module must satisfy all the security requirements specified by the FIPS 140-2 standard. In other words, FIPS 140-2 compliance does not dictate which drives/volumes need to be encrypted; rather it only requires that encrypted volumes must conform to FIPS 140-2 standards. The security requirements for FIPS 140-2 are described in the spec released by NIST.

generated by the Web Conferencing server. The conferencing client then connects to the Web Conferencing server presenting the authentication cookie to be authenticated by the server.

SharePoint Online and OneDrive for Business

All customer content in SharePoint Online is protected by unique, per-file keys that are always exclusive to a single tenant. When a file is uploaded, encryption is performed by SharePoint Online within the context of the upload request, before being sent to Azure storage. When a file is downloaded, SharePoint Online retrieves the encrypted content from Azure storage based on the unique document identifier, and decrypts the content before sending it to the user. Azure storage has no ability to decrypt, or even identify or understand the content. All encryption and decryption happens in the same systems that enforce tenant isolation, which are Azure Active Directory and SharePoint Online.

In SharePoint Online, all content that a customer uploads is encrypted (potentially with multiple AES 256-bit keys) and distributed across the datacenter as follows:[3]

- Each file is broken into one or more chunks, depending on file size. Each chunk is encrypted using its own unique key.
- When a file is updated, the update is handled in the same way: the change is broken into one or more chunks, and each chunk is encrypted with a separate unique key.
- These chunks – files, pieces of files, and update deltas – are stored as blobs in Azure storage that are randomly distributed across multiple Azure storage accounts.
- The set of encryption keys for these chunks of content is itself encrypted using an independently-generated master key.
    - The encrypted keys are stored in the SharePoint Online Content Database.
    - The master key to decrypt the keys to the shreds is stored in a separate secure repository called the Key Store.
- The map used to re-assemble the file is stored in the SharePoint Online Content Database along with the encrypted keys, separately from the master key needed to decrypt them.
- Each Azure storage account has its own unique credentials per access type (read, write, enumerate, and delete). Each set of credentials is held in the secure Key Store and is regularly refreshed.

As described above, there are three different types of stores, each with a distinct function:

- Content is stored as encrypted blobs in Azure storage. The key to each chunk of content is encrypted and stored separately in the Content Database. The content itself holds no clue as to how it can be decrypted.
- The Content Database is a SQL Server database. It holds the map required to locate and reassemble the content blobs held in Azure storage as well as the keys needed to encrypt those blobs. However, the set of keys is itself encrypted. The master key is held in a separate Key Store.

[3] Every step of this encryption is FIPS 140-2 Level 2 validated.

- The Key Store is physically separate from the Content Database and Azure storage. It holds the credentials for each Azure storage container and the master key to the set of encrypted keys held in the Content Database.

Each of these three storage components – the Azure blob store, the Content Database, and the Key Store – is physically separate. The information held in any one of the components is unusable on its own. Without access to all three, it is impossible to retrieve the keys to the chunks, decrypt the keys to make them usable, associate the keys with their corresponding chunks, decrypt each chunk, or reconstruct a document from its constituent chunks.

The master keys, which protect the per-blob keys, are stored in two locations:

- First, a secure repository (the SharePoint Online secret store), which is protected by the Farm Key.
- Second, the master keys are backed-up in the central SharePoint Online secret store.

Currently, these keys are updated (and the blob keys re-encrypted) every 42 days. The credentials used to access the Azure storage containers are also held in the central SharePoint Online secret store, and delegated to each SharePoint Online farm as needed. These credentials are Azure storage SAS signatures, with separate credentials used to read or write data, and with policy applied so that they auto-expire every 60 days. Different credentials are used to read or write data (not both) and SharePoint Online farms are not given permissions to enumerate.

> Note For Office 365 Government customers, data blobs are stored in Azure Government Storage. In addition, access to SharePoint Online keys in Office 365 Government is limited to Office 365 staff has have been specifically screened. Azure Government operations staff do not have access to the SharePoint Online key store that is used for encrypting data blobs.

For more information about data encryption in SharePoint Online and OneDrive for Business, see Data Encryption in OneDrive for Business and SharePoint Online.

List Items in SharePoint Online

List Items are smaller chunks of content that are created ad-hoc or that can live more dynamically within a site, such as rows in a user-created list, individual posts in a SharePoint Online blog, or entries within a SharePoint Online wiki page.

List item contents are encrypted at rest by BitLocker drive encryption, which is enabled on all the back-end and storage servers used by SharePoint Online.

Mailbox-Level Encryption

One of the security principles used by Microsoft in the defense of its cloud services and datacenters is *Assume Breach* – the idea that every component or compartment of a computing system will at some point be compromised by a malicious actor. Assume Breach is a concept that guides security investments, design decisions and operational security practices within Office 365 and all Microsoft

cloud services. For more information about how Microsoft leverages the Assume Breach mindset, see Security Incident Management in Microsoft Office 365. Microsoft's Assume Breach mindset includes Windows administrator accounts and therefore suggests that if some compartmentalization of data access from server administrative access is possible then it should be considered. This conceptual model extends into the realm of data encryption because BitLocker is tied to the Windows access control model and allows an administrator to configure BitLocker, and even disable BitLocker. BitLocker also does not protect data that is copied or moved from an encrypted disk volume to storage media that does not use BitLocker.

More importantly, BitLocker precludes "bring your own key" (BYOK)[4] scenarios that operate at the volume level. BitLocker is a full volume encryption technology that uses a common key across data on the same storage volume. This means that a disk volume that contains data from more than one cloud service tenant would use the same encryption key, thereby precluding scenarios in which a tenant controls encryption keys. To mitigate this threat, Microsoft has compensating controls that prevent any unauthorized copying of data within the service.

To overcome these limitations and enable tenant control and management of encryption keys, Microsoft is adding a feature to Exchange Online known as Mailbox-Level Encryption[5] that includes a BYOK option. The scope for Mailbox-Level Encryption is all customer content[6] that is stored at rest within Exchange Online.[7]

Mailbox-Level Encryption provides multiple benefits. For example, it:

- Enables multi-tenant services to provide per-tenant key management.
- Provides separation of Windows operating system administrators from access to customer content stored or processed by the operating system.
- Provides customers with a mechanism for rendering all customer content inaccessible to Office 365 services upon leaving Office 365.
- Enhances the ability of Office 365 to meet the demands of customers that have requirements regarding encryption.

The implementation of Mailbox-Level Encryption within the Exchange Online application is intended to address the risks and functional limitations of BitLocker. Providing customers with a method to control key material used in the encryption of customer content provides a robust and desirable mechanism for providing customers with the assurance that should the customer choose to leave the Office 365 service that Microsoft will not have continued access to the customer's content. A customer that revokes access to their key material will be able to render all content held within Office

[4] BYOK refers to a method for managing encryption keys which can be applied to several of the technologies discussed in this document.
[5] Previously referred to as Advanced Encryption. See Enhancing transparency and control for Office 365 customers for announcement.
[6] For Exchange Online, all customer content includes everything that an end user generates and stores in their mailbox, including calendar items, notes, tasks, folders, etc. in addition to email messages. For SharePoint Online, this means files.
[7] Skype for Business stores nearly all user-generated content within the user's Exchange Online mailbox and therefore inherits the Mailbox-Level Encryption feature of Exchange Online as it becomes available.

365 unreadable by the cloud service. This is in addition (and a complement) to the Customer Lockbox feature that can be used to control access to customer content by cloud service personnel.

Example Scenario for Mailbox-Level Encryption in Exchange Online with a Customer Managed-Key

Contoso is an Office 365 customer that has elected to use Mailbox-Level Encryption in Exchange Online with a Contoso-managed encryption key. To do this:

1. The Tenant Admin logs into the Contoso Azure subscription to configure encryption keys in Azure Key Vault.
2. The Tenant Admin creates one or more key vaults in their Azure subscription and then imports keys in each key vault using the BYOK toolset; or the Tenant Admin requests a key from Azure Key Vault.
3. The Tenant Admin configures access control using the Azure PowerShell cmdlet Set-AzureKeyVaultAccessPolicy on the key vaults to allow Exchange Online to perform key wrap/unwrap functions.[8]
4. The Tenant Admin creates a data encryption policy for use with Exchange Online mailboxes using the New-DataEncryptionPolicy cmdlet in Remote PowerShell. This data encryption policy will include the URI of the Azure Key Vault key that is to be used with mailboxes that the customer assigns to that encryption key policy. Creation of the encryption policy within Office 365 provides the core information required to validate and begin using the key referenced in the policy.
5. The Tenant Admin uses the Set-Mailbox cmdlet to assign the data encryption policy to one or more Exchange Online mailboxes.
6. Once Office 365 has validated proper configuration of a key policy the service will enable the Tenant Admin to assign objects (mailboxes in the case of Exchange Online) to that key policy.

The following illustration shows the process described above.

[8] See https://msdn.microsoft.com/en-us/library/azure/dn878079.aspx for the operations available for keys and https://msdn.microsoft.com/en-us/library/azure/mt620025.aspx for setting permissions on key vaults.

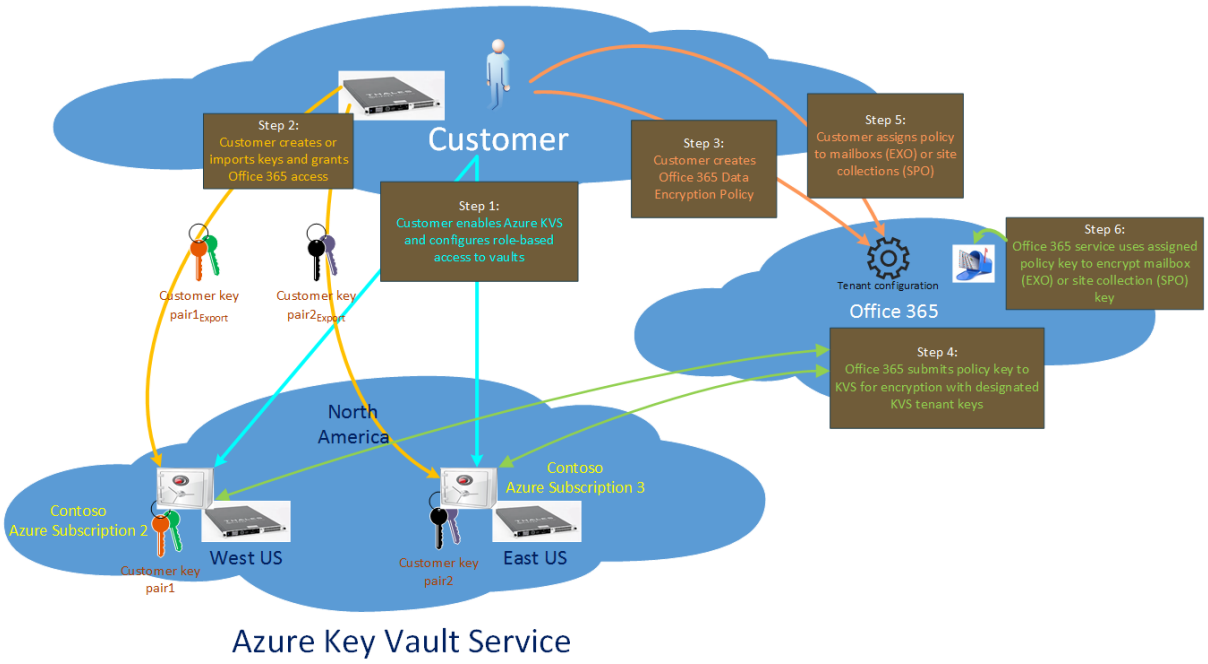

Figure 2 - Enabling Mailbox-Level Encryption with customer-managed keys

An optional step will be to generate or upload multiple keys (not a single key in multiple key vaults) for use with Exchange Online resources, and to create additional encryption key policies for use with those keys. This will allow a tenant to choose, as one example, to assign a key policy that points to an Azure Key Vault key that is held in Europe for resources that are also located in Europe, while using a second key policy that points to an Azure Key Vault key that is held in the United States for resources that are in the United States.

It is expected that every tenant will have a default encryption policy key. For customers that do not choose to own and manage encryption keys, the default policy key will be used to encrypt customer content. If the customer starts using their own encryption key at some point in the future, the act of assigning a data encryption policy (DEP) to service resources would result in the service re-wrapping the existing keys using the newly assigned DEP.

Key Management

There are two scenarios that may require additional key management tasks:

1. You want to stop using an existing key vault that has an associated DEP. In this scenario, you would create a new DEP and assign it to all users.
2. You want to roll the key in the key vault. In this scenario, you would create a new key within, or import a key into, the key vault containing the existing key, perform the process described in Example Scenario for Mailbox-Level Encryption with Customer-Managed Key, and then enable the newly configured key for use by using the Set-DataEncryptionPolicy cmdlet.

When you choose to manage your own key, you control the key that lets Microsoft services decrypt your data. If you delete your key from Azure Key Vault, Office 365 services will eventually lose the ability to function with your data. Microsoft cannot recover your deleted key. To help protect keys managed by your organization, we recommend following these best practices:

- Never purge your keys; only revoke access and only if need be. Removal of a root key without ensuring that 100% of data encryption has been switched to your new key will result in permanent data loss.
- Ensure that you minimize who has permissions to manage your key vault.
- Ensure that your personnel are trained properly.
- Lock your key vault.
- Keep an offline backup of your key just in case your key administrator makes a mistake.

Exiting the Office 365 Service

One of the benefits that Office 365 customers get from using Mailbox-Level Encryption with a customer-managed key is the ability to leave Office 365 and remove access to the encryption key used to encrypt the customer's content, thus rendering all customer content held in Exchange Online inaccessible.

The design for the process of removing access to an encryption key is still under review. Because revocation of access to a key will have major and potentially irreversible effects upon the ability to deliver the affected service(s), Microsoft reserves the right to control when revocation will be honored to allow action to be reversed (in case of mistake, rogue admin, etc.) within a predetermined time.

Encryption of Customer Content In-transit

In addition to protecting customer content at rest, Office 365 uses encryption technologies to protect customer content in-transit. Data is in-transit when a client machine communicates with an Office 365 server, when an Office 365 server communicates with another Office 365 server, or when an Office 365 server communicates with a non-Office 365 (e.g., Exchange Online delivering email to a foreign email server). Inter-datacenter communications between Office 365 servers takes place over TLS or IPsec, and all customer-facing servers negotiate a secure session using TLS with client machines (e.g., Exchange Online uses TLS 1.2 with 256-bit cipher strength is used (FIPS 140-2 Level 2-validated). This applies to the protocols that are used by clients such as Outlook, Skype for Business, and Outlook on the web (e.g., HTTP, POP3, etc.).

The public certificates are issued by Microsoft IT SSL using SSLAdmin, an internal Microsoft tool to protect confidentiality of transmitted information. For information about Microsoft IT certificate authority chaining and operations details, see https://www.microsoft.com/pki/mscorp/cps. All certificates issued by Microsoft IT have a minimum of 2048 bits in length, and Webtrust compliance requires SSLAdmin to make sure that certificates be issued only to public IP addresses owned by Microsoft. Any IP addresses that fail to meet this criterion are routed through an exception process. All the exception requests are handled by the Domains team at Microsoft.

All implementation details such as the version of TLS being used, whether Perfect Forward Secrecy (PFS) is enabled, the order of cipher suites, etc., are available publicly. One way to see these details is to use a third-party Web site, such as Qualys SSL Labs (www.ssllabs.com). Below are the links to automated test pages from Qualys that display information for the following services:

- Office 365 Portal
- Exchange Online
- SharePoint Online
- Skype for Business (SIP)
- Skype for Business (Web)
- Exchange Online Protection

For Exchange Online Protection, URLs vary by tenant names; however, all customers can test Office 365 using microsoft-com.mail.protection.outlook.com.

As for traffic between datacenters, Microsoft deploys applications so that the customer content in this traffic is encrypted using TLS or IPsec. All traffic between Microsoft datacenters is encrypted: this includes both application-layer encryption for the customer content itself, and network transport layer encryption for the communication of the customer content.

Customer-managed Encryption Technologies

Along with the encryption technologies in Office 365 that are managed by Microsoft, Office 365 also includes encryption features that customers can manage and configure. These technologies, which offer a variety of ways to encrypt customer content at rest or in-transit, are:

- Azure Rights Management
- Secure Multipurpose Internet Mail Extension
- Office 365 Message Encryption
- Secure mail flow with a partner organization

Information on these technologies can also be found in the Office 365 service descriptions.

Azure Rights Management

Azure Rights Management (Azure RMS) uses encryption, identity, and authorization policies to help secure your files and email across multiple platforms and devices—phones, tablets, and PCs. Information can be protected both within and outside your organization because protection remains with the data. Azure RMS provides persistent protection of all file types, protects files anywhere, supports business-to-business collaboration, and a wide range of Windows and non-Windows devices. Azure RMS protection can also augment data loss prevention (DLP) policies. But very importantly, authorized people and services (such as search and indexing) can continue to read and inspect the data that Azure RMS protects, which is not easily accomplished with other information protection solutions, such as S/MIME. This ability is sometimes referred to as "reasoning over data" and is a crucial element in maintaining control of your organization's sensitive data.

Azure RMS included in some Office 365 products, and it can also be purchased separately as part of Azure Information Protection by all organizations whether they are using Office 365 or not. Azure RMS is integrated with Office 365 and recommended for all Office 365 customers. To configure Office 365 to use Azure RMS, see Configure IRM to use Azure Rights Management and Set up Information Rights Management (IRM) in SharePoint admin center. If you operate on-premises Active Directory (AD) RMS server then you can also Configure IRM to use an on-premises AD RMS server, but we strongly recommend you to migrate to Azure RMS to use new features like secure collaboration with other organizations.

When you protect content with Azure RMS, Azure RMS uses a 2048-bit RSA asymmetric key with SHA-256 hash algorithm for integrity to encrypt the content. The symmetric key for Office documents and email is AES 128-bit (CBC mode with PKCS#7 padding). For each document or email that is protected by Azure RMS, Azure RMS creates a single AES key (the "content key"), and that key is embedded in the document, and persists through editions of the document. The content key is protected with the organization's RSA key (the "Azure Information Protection tenant key") as part of the policy in the document, and the policy is also signed by the author of the document. This tenant key is common to all documents and emails that are protected by Azure RMS for the organization and this key can only be changed by an Azure Information Protection administrator if the organization is using a tenant key that is customer-managed. For more information about the cryptographic controls used by Azure RMS, see How does Azure RMS work? Under the hood.

In a default Azure RMS implementation, Microsoft generates and manages the root key that is unique for each tenant. Customers can manage the lifecycle of their root key in Azure RMS with Azure Key Vault Services by using a key management method called BYOK that allows you to generate your key in on-premises HSMs, and stay in control of this key after transfer to Microsoft's FIPS 140-2 Level 2-validated HSMs. Access to the root key is not given to any personnel as the keys cannot be exported or extracted from the hardware security modules protecting them. In addition, customers can access a near real-time log showing all access to the root key at any time. For more information, see Logging and Analyzing Azure Rights Management Usage.

Azure Rights Management helps mitigates threats such as wire-tapping, man-in-the-middle attacks, data theft, and unintentional violations of organizational sharing policies. At the same time, any unwarranted access of customer content in-transit or at rest by an unauthorized user who does not have appropriate permissions is prevented via policies that follow that data, thereby mitigating the risk of that data falling in the wrong hands either knowingly or unknowingly and providing data loss prevention functions. If used as part of Azure Information Protection, Azure RMS also provides Data Classification and labeling capabilities, content marking, document access tracking and access revocation capabilities. To learn more about these capabilities, see What is Azure Information Protection.

Secure Multipurpose Internet Mail Extension

Secure/Multipurpose Internet Mail Extensions (S/MIME) is a standard for public key encryption and digital signing of MIME data. S/MIME is defined in RFCs 3369, 3370, 3850, 3851, and others. It allows a user to encrypt an email and digitally sign an email. An email that is encrypted using S/MIME can only be decrypted by the recipient of the email using their private key, which is only available that recipient. As such the emails cannot be decrypted by anybody other than the recipient of the email.

Microsoft supports S/MIME in Office 365. Public certificates are distributed to the customer's on-premises Active Directory and stored in attributes that can be replicated to an Office 365 tenant. The private keys that correspond to the public keys remain on-premises and are never transmitted to Office 365. Users can compose, encrypt, decrypt, read, and digitally sign emails between two users in an organization using Outlook, Outlook on the web, and Exchange ActiveSync clients. For more information, see S/MIME encryption now in Office 365.

Office 365 Message Encryption

Office 365 Message Encryption (OME) is an easy-to-set-up-and-use email service that allows you to send encrypted mail to anyone. OME requires activation of Azure RMS in customer's Office 365 tenant. With OME, tenant administrators can create transport rules that encrypt emails if they match certain criteria. Encrypted messages can be sent inside or outside of customer's tenant. External users can use either an Office 365 account (from their company), a Microsoft account, or a one-time passcode to decrypt the email they have received.

Like Azure Rights Management, OME also mitigates threats such as wire-tapping and man-in-the-middle attacks, and other threats, such as unwarranted access of data by an unauthorized user who does not have appropriate permissions.

Transport Layer Security

If you want to ensure secure communication with a partner, you can use inbound and outbound connectors to provide security and message integrity. You can configure forced inbound and outbound TLS on each connector, using a certificate. Using an encrypted SMTP channel can prevent data from being stolen via a man-in-the-middle attack.

Risks and Protection

Microsoft follows a control and compliance framework that focuses on risks to the Office 365 service and to customer content. Microsoft implements a large set of technology and process-based methods (referred to as *controls*) to mitigate these risks. Identification, evaluation and mitigation of risks via controls is a continuous process. The implementation of controls within various layers of our cloud services such as facilities, network, servers, applications, users (such as Microsoft administrators) and data form a defense-in-depth strategy. The key to this strategy is that many different controls are implemented at different layers to protect against the same or similar risk scenarios. This multi-layered approach provides fail-safe protection in case a control fails for some reason. Some risk scenarios and

the currently available encryption technologies that mitigate them are listed below. These scenarios are in many cases also mitigated via other controls implemented in Office 365.

Encryption Technology	Applies to	Implementation	Risk scenario	Value
BitLocker	Exchange Online, SharePoint Online, Skype for Business	Service implemented	Disks or servers in Office 365 are stolen or improperly recycled.	BitLocker provides a fail-safe approach to protect against loss of data due to stolen or improperly recycled hardware (server / disk).
File-Level Encryption	SharePoint Online	Service implemented	Internal or external hacker tries to access individual files / data as a blob. There is an attempt to access data across tenant.	The encrypted data cannot be decrypted without access to keys. Helps to mitigate risk of a hacker accessing data and cross tenant access of data.
	Skype for Business	Service Implemented	Internal or external hacker tries to access individual files / data as a blob.	The encrypted data cannot be decrypted without access to keys. Helps to mitigate risk of a hacker accessing data.
TLS between Office 365 and clients	Exchange Online, SharePoint Online, Skype for Business, Yammer	Service implemented	Man-in-the-middle or other attack to tap the data flow between Office 365 and client computers over Internet.	This implementation provides value to both Microsoft and customers and assures data integrity as it flows between Office 365 and the client.
TLS between Microsoft datacenters	Exchange Online, SharePoint Online, Skype for Business	Service implemented	Man-in-the-middle or other attack to tap the customer content flow between Office 365 servers located in different Microsoft datacenters.	This implementation is another fail safe method to protect data against attacks between Microsoft datacenters.
Azure Rights Management (included in Office 365 or Azure Information Protection)	Exchange Online, SharePoint Online, and OneDrive for Business	Customer managed	Data falls into the hands of a person who should not have access to the data.	Azure Information Protection uses Azure RMS which provides value to customers by using encryption, identity, and authorization policies to help secure files and email across multiple devices. Azure RMS provides value to customers where all emails originating from Office 365 that match certain criteria (i.e. all emails to a certain address) can be automatically encrypted before they get sent to another recipient.
S/MIME	Exchange Online	Customer managed	Email falls into the hands of a person who is not the intended recipient.	S/MIME provides value to customers by assuring that email encrypted with S/MIME can only be decrypted by the direct recipient of the email.
Office 365 Message Encryption	Exchange Online	Customer managed	Email falls in hands of a person either within or outside Office 365 who is not the intended recipient of the email.	OME provides value to customers where all emails originating from Office 365 that match certain criteria (i.e. all emails to a certain address) are automatically encrypted before they get sent to another internal or an external recipient.
SMTP TLS with partner organization	Exchange Online	Customer managed	Email is intercepted via a man-in-the-middle or other attack while in transit from an Office 365 tenant to another partner organization.	This scenario provides value to the customer such that they can send / receive all emails between their Office 365 tenant and their partner's email organization inside an encrypted SMTP channel.

Table 2 - Risk scenarios and encryption technology mitigation

The following tables summarize the encryption technologies available in Office 365 Multi-tenant and Government Cloud Community environments.

Office 365 Multi-tenant

Encryption Technology	Implemented by	Key Exchange Algorithm and Strength	Key Management[9]	FIPS 140-2 Level 2 Validated
BitLocker	Exchange Online	AES 128-bit+	AES external key is stored in a Secret Safe and in the registry of the Exchange server. The Secret Safe is a secured repository that requires high-level elevation and approvals to access. Access can be requested and approved only by using an internal tool called Lockbox. The AES external key is also stored in the Trusted Platform Module in the server. A 48-digit numerical password is stored in Active Directory and protected by Lockbox.	Yes, for servers that use AES 256-bit[10]
	SharePoint Online	AES 256-bit	AES external key is stored in a Secret Safe. The Secret Safe is a secured repository that requires high-level elevation and approvals to access. Access can be requested and approved only by using an internal tool called Lockbox. The AES external key is also stored in the Trusted Platform Module in the server. A 48-digit numerical password is stored in Active Directory and protected by Lockbox.	Yes
	Skype for Business	AES 256-bit	AES external key is stored in a Secret Safe. The Secret Safe is a secured repository that requires high-level elevation and approvals to access. Access can be requested and approved only by using an internal tool called Lockbox. The AES external key is also stored in the Trusted Platform Module in the server. A 48-digit numerical password is stored in Active Directory and protected by Lockbox.	Yes
File-Level Encryption	SharePoint Online	AES 256-bit	The master keys, which protect the per-blob keys, are stored in two locations: 1. First, the secured store (a built-in SharePoint secret repository) which is protected by the Farm Key. 2. Second, the master keys are backed-up in the central SharePoint Online secret store. These keys are updated (and the blob keys re-encrypted) every 42 days.	Yes
	Skype for Business	AES 256-bit	Each piece of content is encrypted using a different randomly generated 256-bit key. The encryption key is stored in a corresponding metadata XML file which is also encrypted by a per-conference master key. The master key is also randomly generated once per conference.	Yes

[9] TLS certificates referenced in this table are for US datacenters; non-US datacenters also use 2048-bit sha256RSA certificates.

[10] Most servers in the Exchange Online multitenant environment have been deployed with AES 256-bit encryption for BitLocker. Servers using AES 128-bit are being phased out.

Encryption Technology	Implemented by	Key Exchange Algorithm and Strength	Key Management[9]	FIPS 140-2 Level 2 Validated
TLS between Office 365 and clients/partners	Exchange Online	Opportunistic TLS supporting multiple cipher suites	The TLS certificate for Exchange Online (outlook.office.com) is a 2048-bit sha256RSA certificate issued by Baltimore CyberTrust Root. The TLS root certificate for Exchange Online is a 2048-bit sha1RSA certificate issued by Baltimore CyberTrust Root. Be aware that for security reasons, our certificates do change from time to time.	Yes, when TLS 1.2 with 256-bit cipher strength is used
	SharePoint Online		The TLS certificate for SharePoint Online (*.sharepoint.com) is a 2048-bit sha256RSA certificate issued by Baltimore CyberTrust Root. The TLS root certificate for SharePoint Online is a 2048-bit SHA1RSA certificate issued by Baltimore CyberTrust Root. Be aware that for security reasons, our certificates do change from time to time.	Yes
	Skype for Business	TLS for SIP communications and PSOM data sharing sessions	The TLS certificate for Skype for Business (*.lync.com) is a 2048-bit sha256RSA certificate issued by Baltimore CyberTrust Root. The TLS root certificate for Skype for Business is a 2048-bit sha256RSA certificate issued by Baltimore CyberTrust Root.	Yes
TLS between Microsoft datacenters	Exchange Online, SharePoint Online, and Skype for Business	TLS 1.2 with AES 256 Secure Real-time Transport Protocol (SRTP)	Microsoft uses an internally managed and deployed certification authority for server-to-server communications between Microsoft datacenters.	Yes
Azure Rights Management (included in Office 365 or Azure Information Protection)	Exchange Online	Supports Cryptographic Mode 2, an updated and enhanced RMS cryptographic implementation. It supports RSA 2048 for signature and encryption, and SHA-256 for hash in the signature.	Managed by Microsoft.	Yes
	SharePoint Online	Supports Cryptographic Mode 2, an updated and enhanced RMS cryptographic implementation. It supports RSA 2048 for signature and encryption, and SHA-256 for signature.	Managed by Microsoft, which is the default setting; or Customer-managed (aka BYOK), which is an alternative to Microsoft-managed keys. Organization that have an IT-managed Azure subscription can use BYOK and log its usage at no extra charge. For more information, see Implementing bring your own key. In this configuration, Thales HSMs are used to protect your keys. For more information, see Thales HSMs and Azure RMS.	Yes
S/MIME	Exchange Online	Cryptographic Message Syntax Standard 1.5 (PKCS #7)	Depends on the customer-managed public key infrastructure deployed. Key management is performed by the customer, and Microsoft never has access to the private keys used for signing and decryption.	Yes, when configured to encrypt outgoing messages with 3DES or AES256
Office 365 Message Encryption	Exchange Online	Same as Azure RMS (Cryptographic Mode 2 - RSA 2048 for signature and encryption, and SHA-256 for signature)	Uses Azure Information Protection as its encryption infrastructure. The encryption method used depends on where you obtain the RMS keys used to encrypt and decrypt messages.	Yes

Encryption Technology	Implemented by	Key Exchange Algorithm and Strength	Key Management[9]	FIPS 140-2 Level 2 Validated
SMTP TLS with partner organization	Exchange Online	TLS 1.2 with AES 256	The TLS certificate for Exchange Online (outlook.office.com) is a 2048-bit sha256RSA certificate issued by Baltimore CyberTrust Root. The TLS root certificate for Exchange Online is a 2048-bit sha1RSA certificate issued by Baltimore CyberTrust Root. Be aware that for security reasons, our certificates do change from time to time.	Yes, when TLS 1.2 with 256-bit cipher strength is used

Table 3 - Encryption technologies used in Office 365 Multi-tenant

Office 365 Government Community Cloud

Encryption Technology	Implemented by	Key Exchange Algorithm and Strength	Key Management[11]	FIPS 140-2 Level 2 Validated
BitLocker	Exchange Online	AES 256-bit	AES external key is stored in a Secret Safe and in the registry of the Exchange server. The Secret Safe is a secured repository that requires high-level elevation and approvals to access. Access can be requested and approved only by using an internal tool called Lockbox. The AES external key is also stored in the Trusted Platform Module in the server. A 48-digit numerical password is stored in Active Directory and protected by Lockbox.	Yes
	SharePoint Online	AES 256-bit	AES external key is stored in a Secret Safe. The Secret Safe is a secured repository that requires high-level elevation and approvals to access. Access can be requested and approved only by using an internal tool called Lockbox. The AES external key is also stored in the Trusted Platform Module in the server. A 48-digit numerical password is stored in Active Directory and protected by Lockbox.	Yes
	Skype for Business	AES 256-bit	AES external key is stored in a Secret Safe. The Secret Safe is a secured repository that requires high-level elevation and approvals to access. Access can be requested and approved only by using an internal tool called Lockbox. The AES external key is also stored in the Trusted Platform Module in the server. A 48-digit numerical password is stored in Active Directory and protected by Lockbox.	Yes
File-Level Encryption	SharePoint Online	AES 256-bit	The master keys, which protect the per-blob keys, are stored in two locations: 1. First, the secured store (a built-in SharePoint Online secret repository) which is protected by the Farm Key. 2. Second, the master keys are backed-up in the central SharePoint Online secret store. These keys are updated (and the blob keys re-encrypted) every 60 days.	Yes
	Skype for Business	AES 256-bit	Each piece of content is encrypted using a different randomly generated 256-bit key. The encryption key is stored in a corresponding metadata XML file which is also encrypted by a per-conference master key. The master key is also randomly generated once per conference.	Yes

[11] TLS certificates referenced in this table are for US datacenters; non-US datacenters also use 2048-bit sha256RSA certificates.

Encryption Technology	Implemented by	Key Exchange Algorithm and Strength	Key Management[11]	FIPS 140-2 Level 2 Validated
TLS between Office 365 and clients/partners	Exchange Online	Opportunistic TLS supporting multiple cipher suites	The TLS certificate for Exchange Online (outlook.office.com) is a 2048-bit sha256RSA certificate issued by Baltimore CyberTrust Root. The TLS root certificate for Exchange Online is a 2048-bit sha1RSA certificate issued by Baltimore CyberTrust Root. Be aware that for security reasons, our certificates do change from time to time.	Yes, when TLS 1.2 with 256-bit cipher strength is used
	SharePoint Online	TLS 1.2 with AES 256	The TLS certificate for SharePoint Online (*.sharepoint.com) is a 2048-bit sha256RSA certificate issued by Baltimore CyberTrust Root. The TLS root certificate for SharePoint Online is a 2048-bit SHA1RSA certificate issued by Baltimore CyberTrust Root. Be aware that for security reasons, our certificates do change from time to time.	Yes
	Skype for Business	TLS for SIP communications and PSOM data sharing sessions	The TLS certificate for Skype for Business (*.lync.com) is a 2048-bit sha256RSA certificate issued by Baltimore CyberTrust Root. The TLS root certificate for Skype for Business is a 2048-bit sha256RSA certificate issued by Baltimore CyberTrust Root.	Yes
TLS between Microsoft datacenters	Exchange Online, SharePoint Online, and Skype for Business	TLS 1.2 with AES 256 Secure Real-time Transport Protocol (SRTP)	Microsoft uses an internally managed and deployed certification authority for server-to-server communications between Microsoft datacenters.	Yes
Azure Rights Management Service	Exchange Online	Supports Cryptographic Mode 2, an updated and enhanced RMS cryptographic implementation. It supports RSA 2048 for signature and encryption, and SHA-256 for hash in the signature.	Managed by Microsoft.	Yes
	SharePoint Online	Supports Cryptographic Mode 2, an updated and enhanced RMS cryptographic implementation. It supports RSA 2048 for signature and encryption, and SHA-256 for hash in the signature.	Managed by Microsoft, which is the default setting; or Customer-managed (aka BYOK), which is an alternative to Microsoft-managed keys. Organization that have an IT-managed Azure subscription can use BYOK and log its usage at no extra charge. For more information, see Implementing bring your own key. In the BYOK scenario, Thales HSMs are used to protect your keys. For more information, see Thales HSMs and Azure RMS.	Yes
S/MIME	Exchange Online	Cryptographic Message Syntax Standard 1.5 (PKCS #7)	Depends on the public key infrastructure deployed	Yes, when configured to encrypt outgoing messages with 3DES or AES256

Encryption Technology	Implemented by	Key Exchange Algorithm and Strength	Key Management[11]	FIPS 140-2 Level 2 Validated
Office 365 Message Encryption	Exchange Online	Same as Azure RMS (Cryptographic Mode 2 - RSA 2048 for signature and encryption, and SHA-256 for hash in the signature)	Uses Azure RMS as its encryption infrastructure. The encryption method used depends on where you obtain the RMS keys used to encrypt and decrypt messages. If you use Microsoft Azure RMS to obtain the keys, Cryptographic Mode 2 is used. If you use Active Directory (AD) RMS to obtain the keys, either Cryptographic Mode 1 or Cryptographic Mode 2 is used. The method used depends on your on-premises AD RMS deployment. Cryptographic Mode 1 is the original AD RMS cryptographic implementation. It supports RSA 1024 for signature and encryption, and supports SHA-1 for signature. This mode continues to be supported by all current versions of RMS, except for BYOK configurations that use HSMs.	Yes
SMTP TLS with partner organization	Exchange Online	TLS 1.2 with AES 256	The TLS certificate for Exchange Online (outlook.office.com) is a 2048-bit sha256RSA certificate issued by Baltimore CyberTrust Root. The TLS root certificate for Exchange Online is a 2048-bit sha1RSA certificate issued by Baltimore CyberTrust Root. Be aware that for security reasons, our certificates do change from time to time.	Yes

Table 4 - Encryption technologies used in Office 365 Government Cloud Community

Summary

Protection of customer content in Microsoft's cloud services is of paramount importance to Microsoft. Microsoft uses technologies and controlled processes to protect customer content. Within Office 365, customer content is encrypted both at rest and in-transit. Office 365 includes several encryption features that provide content protection out-of-the-box, some of which are customer-managed and some of which are Microsoft-managed. The encryption technologies built into Office 365 and managed by Microsoft protect customer content from a variety of risk scenarios and provide failsafe in case other implemented controls fail to protect customer content. The encryption technologies that are provided to customers enable them to add additional layers of protection to their Office 365 content based on their own risk profiles.

Materials in this Library

Microsoft publishes a variety of content for customers, partners, auditors, and regulators around security, compliance, privacy, and related areas. Below are links to other content in the Office 365 CXP Risk Assurance Documentation library.

Name	Abstract
Auditing and Reporting in Office 365	Describes the auditing and reporting features in Office 365 and Azure Active Directory available to customers. Also details the various audit data that is available to customers via the Office 365 Security & Compliance Center, remote PowerShell, and the Management Activity API. Also describes the internal logging data that is available to Microsoft Office 365 engineers for detection, analysis, and troubleshooting.
Controlling Access to Office 365 and Protecting Content on Devices	Describes the Conditional Access features in Microsoft Office 365 and Microsoft Enterprise Mobility + Security, and how they are designed with built-in data security and protection to keep company data safe while empowering users to be productive on the devices they love. It also provides guidance on how to address common concerns around data access and data protection using Office 365 features.
Content Encryption in Microsoft Office 365	Provides an overview of the various encryption technologies that are used to protect customer content in Office 365, including features deployed and managed by Microsoft and features managed by customers.
Data Resiliency in Office 365	Describes how Microsoft prevents customer content from becoming lost or corrupt in Exchange Online, SharePoint Online, and Skype for Business, and how Office 365 protects customer content from malware and ransomware.
Defending Office 365 Against Denial of Service Attacks	Discusses different types of Denial of Service attacks and how Microsoft defends Office 365, Azure, and their networks against attacks.
Financial Services Compliance in Microsoft's Cloud Services	Describes how the core contract amendments and the Microsoft Regulatory Compliance Program work together to support financial services customers in meeting their regulatory obligations as they relate to the use of cloud services.
Microsoft Threat, Vulnerability, and Risk Assessment of Datacenter Physical Security	Provides an overview regarding the risk assessment of Microsoft datacenters, including potential threats, controls and processes to mitigate threats, and indicated residual risks.
Office 365 Administrative Access Controls	Provides details on Microsoft's approach to administrative access and the controls that are in place to safeguard the services and processes in Office 365. For purposes of this document, Office 365 services include Exchange Online, Exchange Online Protection, SharePoint Online, and Skype for Business. Additional information about some Yammer Enterprise access controls is also included in this document.
Office 365 Customer Security Considerations	Provides organizations with quick access to the security and compliance features in Office 365 and considerations for using them.
Office 365 End of Year Security Report 2014	Covers security and legal enhancements made to Office 365 in calendar year 2014 than enables customers and partners to meet legal requirements surrounding independent verification and audits of Office 365.
Office 365 End of Year Security Report and Pen Test Summary 2015	Office 365 End of Year Security Report and Pen Test Summary for CY 2015.
Office 365 Mapping of CSA Cloud Control Matrix 3.0.1	Provides a detailed overview of how Office 365 maps to the security, privacy, compliance, and risk management controls defined in version 3.0.1-11-24-2015 of the Cloud Security Alliance's Cloud Control Matrix.
Office 365 Risk Management Lifecycle	Provides an overview of how Office 365 identifies, evaluates, and manages identified risks.
Privacy in Office 365	Describes Microsoft's privacy principles and internal privacy standards that guide the collection and use of customer and partner information at Microsoft and give employees a clear framework to help ensure that we manage data responsibly.
Security Incident Management in Microsoft Office 365	Describes how Microsoft handles security incidents in Microsoft Office 365.
Tenant Isolation in Office 365	Describes how Microsoft implements logical isolation of tenant data within Office 365 environment.