Encryption in the Microsoft Cloud

Published: January 2, 2018

This document provides an overview of the various encryption technologies that are currently available in Microsoft's enterprise cloud services, including features deployed and managed by Microsoft and by customers

Table of Contents

Introduction

Customer data within Microsoft's enterprise cloud services is protected by a variety of technologies and processes, including various forms of encryption. Microsoft uses multiple encryption methods, protocols, and ciphers across its products and services to help provide a secure path for customer data to travel through our cloud services, and to help protect the confidentiality of customer data that is stored within our cloud services. Microsoft uses some of the strongest, most secure encryption protocols available to provide barriers against unauthorized access to customer data. Proper key management is also an essential element of encryption best practices, and Microsoft works to ensure that all Microsoft-managed encryption keys are properly secured.

Regardless of customer configuration, customer data stored within Microsoft's enterprise cloud services is protected using one or more forms of encryption.[1] Microsoft provides service-side technologies that encrypt customer data at rest and in transit. For example, for customer data at rest, Microsoft Azure uses BitLocker and DM-Crypt, and Microsoft Office 365[2] uses BitLocker, Azure Storage Service Encryption, Distributed Key Manager (DKM), and Office 365 Service Encryption. For customer data in transit, Azure, Office 365, Microsoft Commercial Support, Microsoft Dynamics 365, Microsoft Power BI, and Visual Studio Team Services use industry-standard secure transport protocols, such as Internet Protocol Security (IPsec) and Transport Layer Security (TLS), between Microsoft datacenters and between user devices and Microsoft datacenters.

In addition to the baseline level of cryptographic security provided by Microsoft, our cloud services also include additional cryptography options that are managed by the customer. For example, customers can enable encryption for traffic between their Azure virtual machines (VMs) and their users. With Azure Virtual Networks, you can use the industry-standard IPsec protocol to encrypt traffic between your corporate VPN gateway and Azure as well as between the VMs located on your Virtual Network. In addition, Office 365 Message Encryption built on top of Azure Information Protection allows you to send encrypted mail to anyone, and Exchange Online Protection (EOP) and Exchange Online support inbound and outbound validation of Domain Keys Identified Mail (DKIM) messages.

In accordance with the Public Key Infrastructure Operational Security Standard, which is a component of the Microsoft Security Policy[3], Microsoft leverages the cryptographic capabilities included in the Windows operating system for certificates and authentication mechanisms, which includes the use of cryptographic modules that meet the U.S. government's Federal Information Processing Standards (FIPS) 140-2 standard.[4]

---

[1] Validation of our crypto policy and its enforcement is independently verified by multiple third-party auditors, and reports of those audits are available on the Service Trust Portal.

[2] Office 365 customer data in this document is defined as Exchange Online mailbox content (e-mail body, calendar entries, and the content of e-mail attachments, and if applicable, Skype for Business content), SharePoint Online site content and the files stored within sites, and files uploaded to OneDrive for Business or Skype for Business.

[3] To access this resource, you must sign in using your cloud service credentials. If you don't have a subscription yet, you can sign up for a free trial.

[4] Relevant NIST certificate numbers for Microsoft can be found at http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm.

FIPS 140-2 is a standard designed specifically for validating product modules that implement cryptography rather than the products that use them. Cryptographic modules that are implemented within a service can be certified as meeting the requirements for hash strength, key management, and the like. Any time cryptographic capabilities are employed to protect the confidentiality, integrity, or availability of data in Microsoft's cloud services, the modules and ciphers used meet the FIPS 140-2 standard.

Microsoft certifies the underlying cryptographic modules used in our cloud services with each new release of the Windows operating system:

- Azure and Azure U.S. Government
- Dynamics 365 and Dynamics 365 U.S. Government
- Office 365, Office 365 U.S. Government, and Office 365 U.S. Government Defense

Encryption in Azure

Technological safeguards in Azure, such as encrypted communications and operational processes, help keep your data secure. You also have the flexibility to implement additional encryption features and manage your own cryptographic keys. Regardless of customer configuration, Microsoft applies encryption to protect customer data in Azure. Microsoft also enables you to control your data hosted in Azure through a range of advanced technologies to encrypt, control and manage cryptographic keys, control and audit access to data. In addition, Azure Storage provides a comprehensive set of security capabilities which together enable developers to build secure applications.

Azure offers many mechanisms for protecting data as it moves from one location to another. Microsoft uses TLS to protect data when it's traveling between the cloud services and customers. Microsoft's datacenters negotiate a TLS connection with client systems that connect to Azure services. Perfect Forward Secrecy (PFS) protects connections between customers' client systems and Microsoft's cloud services by unique keys. Connections also use RSA-based 2,048-bit encryption key lengths. This combination makes it difficult for someone to intercept and access data that is in-transit.

Data can be secured in transit between an application and Azure by using client-side encryption, HTTPS, or SMB 3.0. You can enable encryption for traffic between your own virtual machines (VMs) and your users. With Azure Virtual Networks, you can use the industry-standard IPsec protocol to encrypt traffic between your corporate VPN gateway and Azure as well as between the VMs located on your Virtual Network.

For data at rest, Azure offers many encryption options, such as support for AES-256, giving you the flexibility to choose the data storage scenario that best meets your needs. Data can be automatically encrypted when written to Azure Storage using Storage Service Encryption, and operating system and data disks used by VMs can be encrypted using Azure Disk Encryption. In addition, delegated access to data objects in Azure Storage can be granted using Shared Access Signatures. Azure also provides encryption for data at rest using Transparent Data Encryption for Azure SQL Database and Data Warehouse.

For more information about encryption in Azure, see Azure encryption overview and Azure Data Encryption-at-Rest.

Azure Disk Encryption

Azure Disk Encryption enables you to encrypt your Windows and Linux Infrastructure as a Service (IaaS) VM disks. Azure Disk Encryption leverages the BitLocker feature of Windows and the DM-Crypt feature of Linux to provide volume-level encryption for the operating system and the data disks. It also ensures that all data on the VM disks are encrypted at rest in your Azure storage. Azure Disk Encryption is integrated with Azure Key Vault to help you control, manage, and audit the use of the encryption keys and secrets.

For more information, see Azure Disk Encryption for Windows and Linux IaaS VMs.

Azure Storage Service Encryption

With Azure Storage Service Encryption, Azure Storage automatically encrypts data prior to persisting it to storage and decrypts data prior to retrieval. The encryption, decryption, and key management processes are totally transparent to users. Azure Storage Service Encryption can be used for Azure Blob Storage and Azure Files. You can also use Microsoft-managed encryption keys with Azure Storage Service Encryption, or you can use your own encryption keys.[5] In addition, you can automate the use of encryption. For example, you can programmatically enable or disable Storage Service Encryption on a storage account using the Azure Storage Resource Provider REST API, the Storage Resource Provider Client Library for .NET, Azure PowerShell, or the Azure CLI.

Some Office 365 services use Azure for storing data. For example, SharePoint Online and OneDrive for Business store data in Azure Blob storage, and Microsoft Teams stores data for its chat service in tables, blobs, and queues. In addition, the Compliance Manager feature of the Service Trust Portal stores customer-entered data which is stored in encrypted form in Azure Cosmos DB, a Platform as a Service (PaaS), globally-distributed, multi-model database. Azure Storage Service Encryption encrypts data stored in Azure Blob storage and in tables, and Azure Disk Encryption encrypts data in queues, as well as Windows and IaaS virtual machine disks to provide volume encryption for the operating system and the data disk. The solution ensures that all data on the virtual machine disks are encrypted at rest in your Azure storage. Encryption at rest in Azure Cosmos DB is implemented by using several security technologies, including secure key storage systems, encrypted networks, and cryptographic APIs.

Azure Key Vault

Secure key management is not just core to encryption best practices; it's also essential for protecting data in the cloud. Azure Key Vault enables you to encrypt keys and small secrets like passwords that use keys stored in hardware security modules (HSMs). Azure Key Vault is Microsoft's recommended solution for managing and controlling access to encryption keys used by cloud services. Permissions

[5] For information on using your own keys, see Storage Service Encryption using customer managed keys in Azure Key Vault. For information about using Microsoft-managed keys, see Storage Service Encryption for Data at Rest.

to access keys can be assigned to services or to users with Azure Active Directory accounts. Azure Key Vault relieves organizations of the need to configure, patch, and maintain HSMs and key management software. With Azure Key Vault, Microsoft never sees your keys and applications don't have direct access to them; you maintain control. You can also import or generate keys in HSMs. Organizations that have a subscription that includes Azure Information Protection can configure their Azure Information Protection tenant to use a customer-managed key (BYOK) and log its usage.

Encryption in Office 365

Encryption of Office 365 customer data at rest is provided by multiple service-side technologies, including BitLocker, DKM, Azure Storage Service Encryption, and service encryption in Exchange Online, Skype for Business, OneDrive for Business, and SharePoint Online. Office 365 Service Encryption include an option to use customer-managed encryption keys that are stored in Azure Key Vault. This customer-managed key option, called Office 365 Customer Key, is available for Exchange Online, SharePoint Online, and OneDrive for Business.

For customer data in transit, all Office 365 servers negotiate secure sessions using TLS by default with client machines to secure customer data.[6] This applies to protocols on any device used by clients, such as Skype for Business, Outlook, and Outlook on the web, mobile clients, and web browsers.

BitLocker

Office 365 servers use BitLocker to encrypt the disk drives containing customer data 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 data. 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 data in Exchange Online, SharePoint Online, and Skype for Business. Disk sectors are encrypted with a Full Volume Encryption Key (FVEK), which is 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 following figure illustrates an example of the BitLocker key protection chain for a given server (in this case, using an Exchange Online server).

[6] All customer-facing servers negotiate to TLS 1.2 by default, but we also support negotiating down to a lower standard, if required.

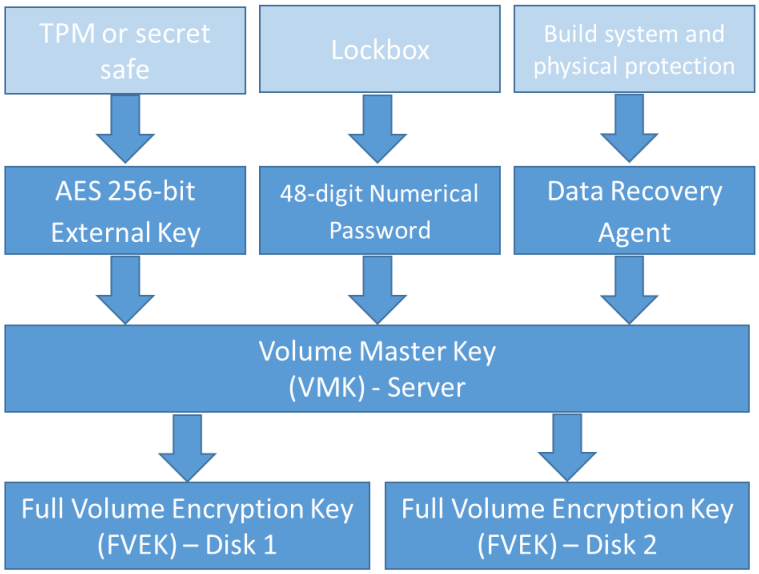

Figure 1 - BitLocker Protection Chain for Exchange Online servers

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 the private key. 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.

BitLocker supports keys which 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 to a given 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 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 FIPS-compliant algorithms to ensure that encryption keys are never stored or sent over the wire in the clear. The Office 365 implementation of customer data-at-rest-protection does not deviate from the default BitLocker implementation.

Distributed Key Manager

Distributed Key Manager (DKM) is a client-side functionality that uses a set of secret keys to encrypt and decrypt information. Only members of a specific security group in Active Directory Domain Services can access those keys to decrypt the data that is encrypted by DKM. In Exchange Online, only certain service accounts under which the Exchange processes run are part of that security group. As part of standard operating procedure in the datacenter, no human is given credentials that are part of this security group and therefore no human has access to the keys that can decrypt these secrets.

Within Office 365, Microsoft uses DKM for the Rights Management service (RMS) root keys. These are customer keys that are either imported from Azure RMS or from a customer's on-premises Active Directory RMS deployment that is used for encrypting and decrypting emails with RMS or Office 365 Message Encryption (OME).

Office 365 Service Encryption

In addition to using volume-level encryption, Exchange Online, Skype for Business, SharePoint Online, and OneDrive for Business also use Service Encryption to encrypt customer data. Service Encryption allows for two key management options:

- Microsoft manages all cryptographic keys.[7]
- The customer supplies root keys used with service encryption and the customer manages these keys using Azure Key Vault. Microsoft manages all other keys. This option is called Customer Key, and it is currently available for Exchange Online, SharePoint Online, and OneDrive for Business.[8]

Service encryption provides multiple benefits. For example, it:

- Provides rights protection and management features on top of strong encryption protection.
- Includes a Customer Key option that enables multi-tenant services to provide per-tenant key management.
- Provides separation of Windows operating system administrators from access to customer data stored or processed by the operating system.

[7] This option is currently available in SharePoint Online, OneDrive for Business, and Skype for Business. It is currently on the roadmap for Exchange Online.
[8] Previously referred to as Advanced Encryption with BYOK. See Enhancing transparency and control for Office 365 customers for the original announcement.

- Enhances the ability of Office 365 to meet the demands of customers that have compliance requirements regarding encryption.

Customer Key

Using Customer Key, you can generate your own cryptographic keys using either an on-premises HSM or Azure Key Vault. Regardless of how the key is generated, customers use Azure Key Vault to control and manage the cryptographic keys used by Office 365. Once your keys are stored in Azure Key Vault, they can be assigned to workloads such as Exchange Online and SharePoint Online and used to as the root of the keychain used to encrypt your mailbox data and files.

One of the other benefits of using Customer Key is to control the ability of Microsoft to process customer data. This capability exists so that a customer that wants to remove data from Office 365 (such as when a customer terminates service with Microsoft or removes a portion of data stored in the cloud) can do so and use Customer Key as a technical control to ensure that no one, including Microsoft, can access or process the data. This is in addition (and a complement) to the Customer Lockbox feature that can be used to control access to customer data by Microsoft personnel.

To learn how to set up Customer Key for Office 365 for Exchange Online, Skype for Business, SharePoint Online, and OneDrive for Business, see Controlling your data in Office 365 using Customer Key. For additional information, see the Customer Key for Office 365 FAQ, and Manage and control your data to help meet compliance needs with Customer Key.

Skype for Business

Skype for Business customer data may be stored at rest in the form of files or presentations that are uploaded by meeting participants. The Web Conferencing server encrypts customer data using AES with a 256-bit key. The encrypted customer data is stored on a file share. Each piece of customer data is encrypted using a different randomly generated 256-bit key. When a piece of customer data is shared in a conference, the Web Conferencing server instructs the conferencing clients to download the encrypted customer data via HTTPS. It sends the corresponding key to clients so that the customer data can be decrypted. The Web Conferencing server also authenticates conferencing clients before it allows the clients access to conference customer data. 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 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

All customer files in SharePoint Online are protected by unique, per-file keys that are always exclusive to a single tenant. The keys are either created and managed by the SharePoint Online service, or when Customer Key is used, created and managed by customers. 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 customer data from Azure storage based on the unique document identifier and decrypts the customer data before sending it to the user. Azure storage has no ability to decrypt, or even identify or understand the customer data. All encryption and decryption happen in the same systems that enforce tenant isolation, which are Azure Active Directory and SharePoint Online.

Several workloads in Office 365 store data in SharePoint Online, including Microsoft Teams, which stores all files in SharePoint Online, and OneDrive for Business, which uses SharePoint Online for its storage. All customer data stored in SharePoint Online is encrypted (with one or more AES 256-bit keys) and distributed across the datacenter as follows:[9]

- Each file is split into one or more chunks, depending on file size. Each chunk is encrypted using its own unique AES 256-bit key.
- When a file is updated, the update is handled in the same way: the change is split 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 customer data is itself encrypted.
    - The keys used to encrypt the blobs are stored in the SharePoint Online Content Database.
    - The Content Database is protected by database access controls and encryption at rest. Encryption is performed using Transparent Data Encryption (TDE) in Azure SQL Database[10]. These secrets are at the service level for SharePoint Online, not at the tenant level. These secrets (sometimes referred to as the master keys) are stored in a separate secure repository called the Key Store. TDE provides security at rest for both the active database and the database backups and transaction logs.
    - When customers provide the optional key, the customer key is stored in Azure Key Vault, and the service uses the key to encrypt a tenant key, which is used to encrypt a site key, which is then used to encrypt the file level keys. Essentially, a new key hierarchy is introduced when the customer provides a key.
- The map used to re-assemble the file is stored in the 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:

- Customer data is stored as encrypted blobs in Azure storage. The key to each chunk of customer data is encrypted and stored separately in the Content Database. The customer data itself holds no clue as to how it can be decrypted.

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

[10] Azure SQL Database is a general-purpose relational database service in Microsoft Azure that supports structures such as relational data, JSON, spatial, and XML.

- The Content Database is a SQL Server database. It holds the map required to locate and reassemble the customer data blobs held in Azure storage as well as the keys needed to encrypt those blobs. However, the set of keys is itself encrypted (as explained above) and held in a separate Key Store.
- 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.

BitLocker certificates, which protect the physical disk volumes on machines in the datacenter, are stored in a secure repository (the SharePoint Online secret store) that is protected by the Farm key.

The TDE keys that protect the per-blob keys are stored in two locations:

- The secure repository, which houses the BitLocker certificates and is protected by the Farm Key; and
- In a secure repository managed by Azure SQL Database.

The credentials used to access the Azure storage containers are also held in the 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 U.S. Government customers, data blobs are stored in Azure U.S. Government Storage. In addition, access to SharePoint Online keys in Office 365 U.S. Government is limited to Office 365 staff that have been specifically screened. Azure U.S. 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 customer data 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 items are stored in the Content Database (Azure SQL Database) and protected with TDE.

Exchange Online

Exchange Online uses BitLocker for all mailbox data, and the BitLocker configuration is described above. To provide an additional layer of encryption, Microsoft also provides service encryption for Exchange Online, which results in all mailbox data being encrypted at the mailbox level by Exchange Online. Currently available is the version of service encryption that uses a customer-managed key (Customer Key).[11] This method of encryption provides increased protection not afforded by BitLocker because it provides separation of server administrators and the cryptographic keys necessary for decryption of data, and because the encryption is applied directly to the data (in contrast with BitLocker, which applies encryption at the logical disk volume) any customer data copied from an Exchange server remains encrypted.

The scope for Exchange Online service encryption is customer data that is stored at rest within Exchange Online.[12]

Encryption of Office 365 customer data in transit

In addition to protecting customer data at rest, Microsoft uses encryption technologies to protect Office 365 customer data 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; and
- When an Office 365 server communicates with a non-Office 365 server (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[13]). 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.[14] All certificates issued by Microsoft IT have a minimum of 2048 bits in length, and Webtrust compliance requires SSLAdmin to make sure that certificates are 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 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

[11] A Microsoft-managed key option for Exchange Online service encryption is also on Microsoft's roadmap.
[12] Skype for Business stores nearly all user-generated content within the user's Exchange Online mailbox and therefore inherits the service encryption feature of Exchange Online.
[13] See Technical reference details about encryption in Office 365 for a list of TLS cipher suites supported by Office 365.
[14] For information about Microsoft IT certificate authority chaining and operations details, see https://www.microsoft.com/pki/mscorp/cps.

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
- Microsoft Teams

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

Customer-managed encryption features in Office 365

Along with the encryption technologies and features in Office 365 that are described above, Office 365 also includes additional encryption features that customers can manage and configure, including:

- Azure Rights Management
- Secure Multipurpose Internet Mail Extension
- Office 365 Message Encryption
- Domain Keys Identified Mail (DKIM)
- Secure mail flow with a partner organization

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

Azure Rights Management

Azure Rights Management (Azure RMS) is the protection technology used by Azure Information Protection. 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. For more information about which applications and services can use the Azure Rights Management service from Azure Information Protection, see How applications support the Azure Rights Management service.

Azure RMS is integrated with Office 365 and available to 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 customer data with Azure RMS, Azure RMS uses a 2048-bit RSA asymmetric key with SHA-256 hash algorithm for integrity to encrypt the data. 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 data 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, Azure Information Protection deployment roadmap, and Quick start tutorial for 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 to 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) built on top of Azure Information Protection (AIP) enables you to send encrypted and rights-protected mail to anyone. OME 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. We have made investments that provide you with a simpler, more intuitive, secure email experience built on top of Azure Information Protection. You can protect messages sent from Office 365 to anyone inside or outside your organization. These messages can be viewed across a diverse set of mail clients using any identity, including Azure Active Directory, Microsoft Account, and Google IDs. For more information on how your organization can use encrypted messages, see the following resources:

- Send, view, and reply to encrypted messages in Outlook for PC
- Office 365 Message Encryption capabilities built on top of Azure Information Protection
- Planning and implementing your Azure Information Protection tenant key
- Define mail flow rules to encrypt email messages in Office 365

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. For more information, see Set up connectors for secure mail flow with a partner organization.

Domain Keys Identified Mail

Exchange Online Protection (EOP) and Exchange Online support inbound validation of Domain Keys Identified Mail (DKIM) messages. DKIM is a method for validating that a message was sent from the domain it says it originated from and that it was not spoofed by someone else. It ties an email message to the organization responsible for sending it. DKIM verification is automatically used for all messages sent over IPv6 communications.[15]

DKIM validates a digitally signed message that appears in the DKIM-Signature header in the message headers. The results of a DKIM-Signature validation are stamped in the Authentication-Results header that conforms to RFC7001 - Message Header Field for Indicating Message Authentication Status. The message header text appears like the following (where contoso.com is the sender):

```
Authentication-Results: <contoso.com>; dkim=pass (signature was verified) header.d=example.com;
```

[15] For more information about IPv6 support, see Support for anonymous inbound email messages over IPv6.

Exchange Online also supports the creation of mail flow rules based on the results of a DKIM validation, which can be used to filter or route messages as needed.

Risks and Protection for Office 365

Microsoft follows a control and compliance framework that focuses on risks to the Office 365 service and to customer data. 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	Services	Key Management	Risk scenario	Value
BitLocker	Exchange Online, SharePoint Online, and Skype for Business	Microsoft	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).
Service Encryption	SharePoint Online, Skype for Business, and OneDrive for Business; Exchange Online: (on roadmap)	Microsoft	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.
Customer Key	SharePoint Online, Exchange Online, and Skype for Business	Customer	N / A[16]	Helps customers meet internal regulation and compliance obligations, and the ability to leave the Office 365 service and revoke Microsoft's access to data
TLS between Office 365 and clients	Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Teams, and Yammer	Microsoft, Customer	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, OneDrive for Business, and Skype for Business	Microsoft	Man-in-the-middle or other attack to tap the customer data flow between Office 365 servers located in different Microsoft datacenters.	This implementation is another 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	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

[16] This feature is designed as a compliance feature; not as a mitigation for any risk.

Encryption Technology	Services	Key Management	Risk scenario	Value
				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	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	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	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.

Encryption Technology	Implemented by	Key Exchange Algorithm and Strength	Key Management[17]	FIPS 140-2 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[18]
	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

[17] TLS certificates referenced in this table are for US datacenters; non-US datacenters also use 2048-bit SHA256RSA certificates.

[18] Most servers in the Exchange Online multi-tenant 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[17]	FIPS 140-2 Validated
	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
Service Encryption	SharePoint Online	AES 256-bit	The keys used to encrypt the blobs are stored in the SharePoint Online Content Database. The SharePoint Online Content Databases is protected by database access controls and encryption at rest. Encryption is performed using TDE in Azure SQL Database. These secrets are at the service level for SharePoint Online, not at the tenant level. These secrets (sometimes referred to as the master keys) are stored in a separate secure repository called the Key Store. TDE provides security at rest for both the active database and the database backups and transaction logs. When customers provide the optional key, the customer key is stored in Azure Key Vault, and the service uses the key to encrypt a tenant key, which is used to encrypt a site key, which is then used to encrypt the file level keys. Essentially, a new key hierarchy is introduced when the customer provides a key.	Yes
	Skype for Business	AES 256-bit	Each piece of data 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
	Exchange Online	AES 256-bit	Each mailbox is encrypted using a data encryption policy that uses encryption keys controlled by Microsoft (on roadmap) or by the customer (when Customer Key is used).	Yes
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.	Yes, when TLS 1.2 with 256-bit cipher strength is used
	SharePoint Online	TLS 1.2 with AES 256 Data Encryption in OneDrive for Business and 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.	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
	Microsoft Teams	TLS 1.2 with AES 256 Frequently asked questions about Microsoft Teams – Admin Help	The TLS certificate for Microsoft Teams (teams.microsoft.com, edge.skype.com) is a 2048-bit SHA256RSA certificate issued by Baltimore CyberTrust Root. The TLS root certificate for Microsoft Teams is a 2048-bit SHA256RSA certificate issued by Baltimore CyberTrust Root.	Yes

Encryption Technology	Implemented by	Key Exchange Algorithm and Strength	Key Management[17]	FIPS 140-2 Validated
TLS between Microsoft datacenters	All Office 365 services	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, 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
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.	Yes, when TLS 1.2 with 256-bit cipher strength is used

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

Encryption Technology	Implemented by	Key Exchange Algorithm and Strength	Key Management[19]	FIPS 140-2 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

[19] 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[19]	FIPS 140-2 Validated
	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
Service Encryption	SharePoint Online	AES 256-bit	The keys used to encrypt the blobs are stored in the SharePoint Online Content Database. The SharePoint Online Content Databases is protected by database access controls and encryption at rest. Encryption is performed using TDE in Azure SQL Database. These secrets are at the service level for SharePoint Online, not at the tenant level. These secrets (sometimes referred to as the master keys) are stored in a separate secure repository called the Key Store. TDE provides security at rest for both the active database and the database backups and transaction logs. When customers provide the optional key, the Customer Key is stored in Azure Key Vault, and the service uses the key to encrypt a tenant key, which is used to encrypt a site key, which is then used to encrypt the file level keys. Essentially, a new key hierarchy is introduced when the customer provides a key.	Yes
	Skype for Business	AES 256-bit	Each piece of data 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
	Exchange Online	AES 256-bit	Each mailbox is encrypted using a data encryption policy that uses encryption keys controlled by Microsoft or by the customer (when Customer Key is used).	Yes
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.	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.	Yes

Encryption Technology	Implemented by	Key Exchange Algorithm and Strength	Key Management[19]	FIPS 140-2 Validated
	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
	Microsoft Teams	Frequently asked questions about Microsoft Teams – Admin Help	The TLS certificate for Microsoft Teams (teams.microsoft.com; edge.skype.com) is a 2048-bit SHA256RSA certificate issued by Baltimore CyberTrust Root. The TLS root certificate for Microsoft Teams is a 2048-bit SHA256RSA certificate issued by Baltimore CyberTrust Root.	Yes
TLS between Microsoft datacenters	Exchange Online, SharePoint Online, 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 AES-256.

Encryption Technology	Implemented by	Key Exchange Algorithm and Strength	Key Management[19]	FIPS 140-2 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

Encryption in Microsoft Dynamics 365

Microsoft uses encryption technology to protect customer data in Dynamics 365 while at rest in a Microsoft database and while it is in transit between user devices and our datacenters. Connections established between customers and Microsoft datacenters are encrypted, and all public endpoints are secured using industry-standard TLS. TLS effectively establishes a security-enhanced browser-to-server connection to help ensure data confidentiality and integrity between desktops and datacenters. After data encryption is activated, it cannot be turned off.[20]

Dynamics 365 uses standard Microsoft SQL Server cell level encryption for a set of default entity attributes that contain sensitive information, such as user names and email passwords. This feature can help organizations meet the compliance requirements associated with FIPS 140-2. Field-level data encryption is especially important in scenarios that leverage the Microsoft Dynamics CRM Email Router, which must store user names and passwords to enable integration between a Dynamics 365 instance and an email service.

All instances of Dynamics 365 use Microsoft SQL Server Transparent Data Encryption (TDE) to perform real-time encryption of data when written to disk (at rest). TDE encrypts SQL Server, Azure SQL Database, and Azure SQL Data Warehouse data files. By default, Microsoft stores and manages

[20] For more information, see Field-level data encryption.

the database encryption keys for your instances of Dynamics 365.[21] The manage keys feature in the Dynamics 365 Administration Center gives administrators the ability to self-manage the database encryption keys that are associated with instances of Dynamics 365.[22] The key management feature supports both PFX and BYOK encryption key files, such as those stored in an HSM.[23] To use the upload encryption key option you need both the public and private encryption key.

The key management feature takes the complexity out of encryption key management by using Azure Key Vault to securely store encryption keys. Azure Key Vault helps safeguard cryptographic keys and secrets used by cloud applications and services. The key management feature doesn't require that you have an Azure Key Vault subscription and for most situations there is no need to access encryption keys used for Dynamics 365 within the vault.

Summary

Customer data within Microsoft's enterprise cloud services is protected by a variety of technologies and processes, including various forms of encryption. Regardless of customer configuration, customer data stored within Microsoft's cloud services is protected using encryption. Microsoft provides service-side technologies that encrypt customer data at rest and in transit. For example, for customer data at rest, Azure uses BitLocker and DM-Crypt, and Office 365 uses BitLocker, Azure Storage Service Encryption, and Office 365 Service Encryption. For customer data in transit, Azure, Office 365, Microsoft Commercial Support, Dynamics 365, Power BI, and Visual Studio Team Services use industry-standard secure transport protocols, such as IPsec and TLS, between user devices and Microsoft datacenters. In addition to the baseline level of cryptographic security provided by Microsoft, our cloud services also include additional cryptography options that are managed by the customer.

Further Reading

Microsoft delivers key information about its enterprise cloud services through a library of deep dive transparency whitepapers that describe how Microsoft has built and operated its cloud services. These documents cover the following topics:

- Tenant Isolation
- Conditional Access
- Administrative Access Controls
- Data Resiliency
- Defending against denial-of-service attacks
- Security Incident Management
- Auditing and Reporting

[21] The keys that are used by Dynamics 365 for Financials are generated by the .NET Framework Data Protection API.
[22] Self-managed database encryption keys are only available in the January 2017 update for Microsoft Dynamics 365 and may not be made available for later versions. For more information, see Manage the encryption keys for your Dynamics 365 (online) instance.
[23] For more information about generating and transferring an HSM-protected key over the Internet see How to generate and transfer HSM-protected keys for Azure Key Vault.