

Microsoft 365 en encryptie

17 December 2024



Albert Hoitingh

Principal consultant @ InSpark



Microsoft 365 | Security



@Alberthoitingh



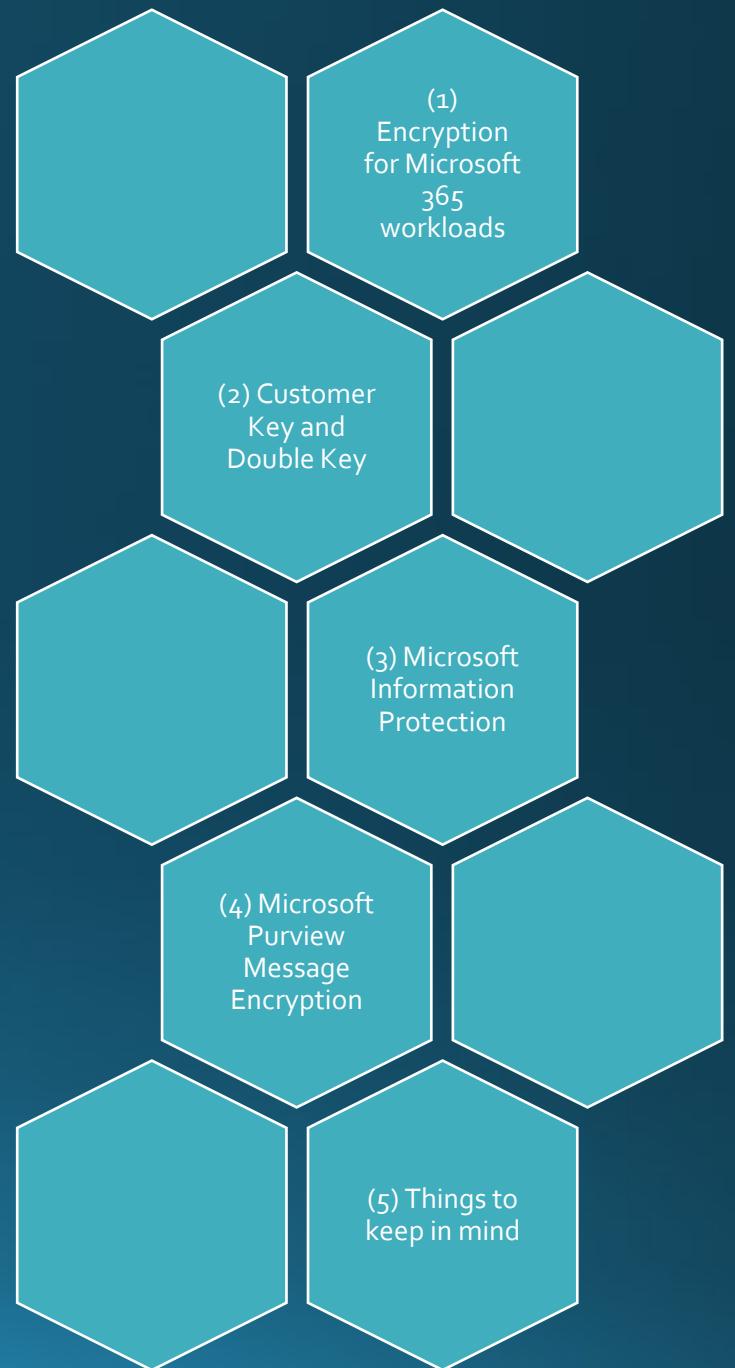
<https://linkedin.com/in/appieh>



<https://alberthoitingh.com>

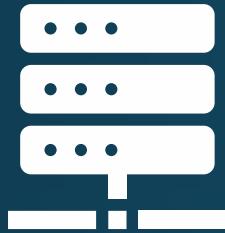


Today's agenda



Encryption in Microsoft 365 and Purview

Different scopes



1

At rest



2

In transit



3

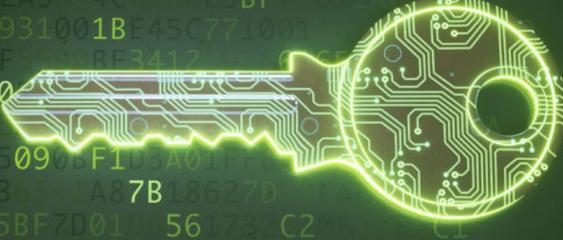
Specific functions

Short side note...

Microsoft | Research | Our research | Programs & events | Connect & learn | About | Register: Research Forum | All Microsoft | Search

Microsoft SEAL

Build end-to-end encrypted data storage and computation services



Overview | Release news | People | Publications | Videos | News & features

Microsoft SEAL—powered by open-source homomorphic encryption technology—provides a set of encryption libraries that allow computations to be performed directly on encrypted data. This enables software engineers to build end-to-end encrypted data storage and computation services where the customer never needs to share their key with the service.

Microsoft SEAL is open source (MIT license). Start using it today!

[Download](#)

Citing Microsoft SEAL | Contact us

Homomorphic Encryption

Homomorphic Encryption refers to a [new type of encryption technology](#) that allows computation to be directly on encrypted data, without requiring any decryption in the process. The first homomorphic encryption scheme was invented in 2009 and several improved schemes were created over the following years. There were a few notable and publicly available implementations, but their use required extensive understanding of the complicated mathematics underlying homomorphic encryption and were not easily usable by normal software developers.

Our goal was different: making homomorphic encryption easy to use and available for *everyone*. Today, Microsoft SEAL reaches this goal by providing a simple and convenient API with state-of-the-art performance. Microsoft SEAL comes with several detailed and thoroughly commented examples, demonstrating how the library can be used correctly and securely, and explaining any necessary background material.

Short side note...



CISA INSIGHTS

Preparing Critical Infrastructure for Post-Quantum Cryptography

August 2022

Quantum Risk to Digital Communications

Nation-states and private companies are actively pursuing the capabilities of quantum computers. Quantum computing opens up exciting new possibilities; however, the consequences of this new technology include threats to the current cryptographic standards. These standards ensure data confidentiality and integrity and support key elements of network security. While quantum computing technology capable of breaking public key encryption algorithms in the current standards does not yet exist, government and critical infrastructure entities—including both public and private organizations—must work together to prepare for a new post-quantum cryptographic standard to defend against future threats.

In March 2021, Secretary of Homeland Security Alejandro N. Mayorkas [outlined his vision for cybersecurity resilience](#) and identified the transition to post-quantum encryption as a priority. Government and critical infrastructure organizations must take coordinated preparatory actions now to ensure a fluid migration to the new post-quantum cryptographic standard that the National Institute of Standards and Technology (NIST) will publish in 2024.

Conducting an inventory of vulnerable critical infrastructure systems across the [55 National Critical Functions \(NCFs\)](#) is the first step of this preparation and is included in the [Post-Quantum Cryptography Roadmap](#) developed by DHS and NIST. There are potential risks from quantum computing to each of the 55 NCFs. CISA urges asset owners and operators to follow the [Roadmap](#) and [CISA's Post-Quantum Cryptography Initiative webpage](#) to begin the process of addressing this risk within their organization.

The Quantum Threat to Public Key Cryptography

All digital communications—email, online banking, online messaging, etc.—rely on data encryption built into the devices and applications used to transmit data. This encryption is based on mathematical functions that secure data in transit, protecting the data from tampering or espionage. In public key encryption (also known as asymmetric encryption), the mathematical functions rely on cryptographic keys to encrypt data and authenticate the sender and recipient.

Public key encryption requires that each message use two separate, but related keys (one is called a public key and the other is called a private key) to protect data. The sender and recipient of the data do not share their private keys, while public keys can be shared without downgrading the level of cryptographic security. The sender uses their private key to encode the message and provides the recipient with their public key to decode the message. To reply, the recipient will follow the same procedure and share their public key.

Because only two keys can decode a message, digital signatures allow a party to sign a message with their private key while verifiers use the public key to authenticate that the sender actually sent the message. All organizations regularly use public key cryptography to securely send emails, verify digital signatures, secure sensitive data, and protect user information online.

When quantum computers reach higher levels of computing power and speed, they will be capable of breaking

Cyberwarfare / Nation-State Attacks , Encryption & Key Management , Fraud Management & Cybercrime

US Government Picks Quantum-Resistant Encryption Algorithms

Quantum Computers That Use Atom-Level States of Uncertainty Are a Matter of Time

David Perera (@daveperera) • July 5, 2022

[Email](#) [Print](#) [Briefcase](#) [Twitter](#) [Facebook](#) [LinkedIn](#) [Credit Eligible](#)

[Get Permission](#)



Licensing considerations



1

Basic functions



2

eDiscovery (Premium)



3

Customer Key
Double Key Encryption
Advanced Managed Encryption

Data at rest

BitLocker – on many levels

Per-file encryption (SPO)

Data Encryption Policies (DEPs)

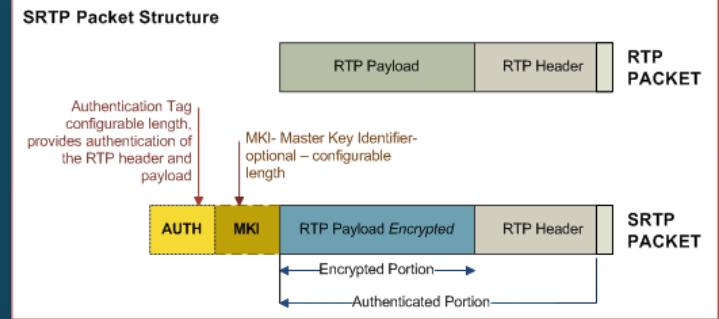
SharePoint Online and OneDrive

Exchange Online

All other Microsoft 365 services, incl. Microsoft Purview
Information Protection



Data in transit



<https://www.adaptivedigital.com/secure-rtp/>

(Mutual) Transport Layer Security (MTLS/TLS)

Secure Real-Time Transport Protocol (SRTP)

Exchange IRM – s/MIME – OME



Key management

Key management



1

Microsoft managed



2

Customer Key

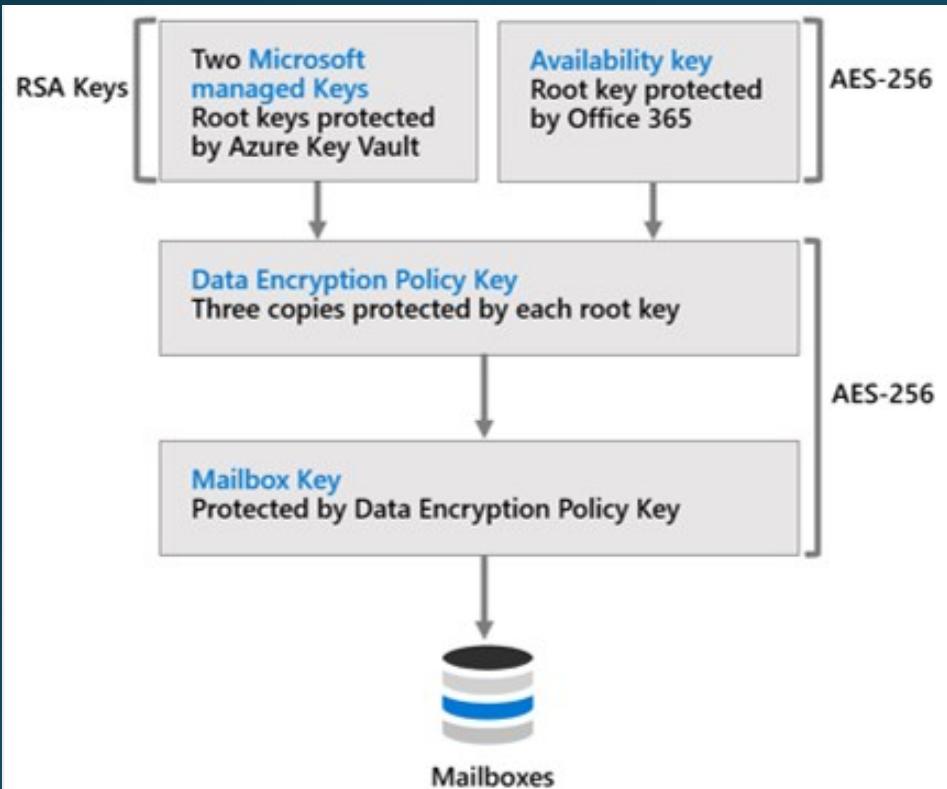


3

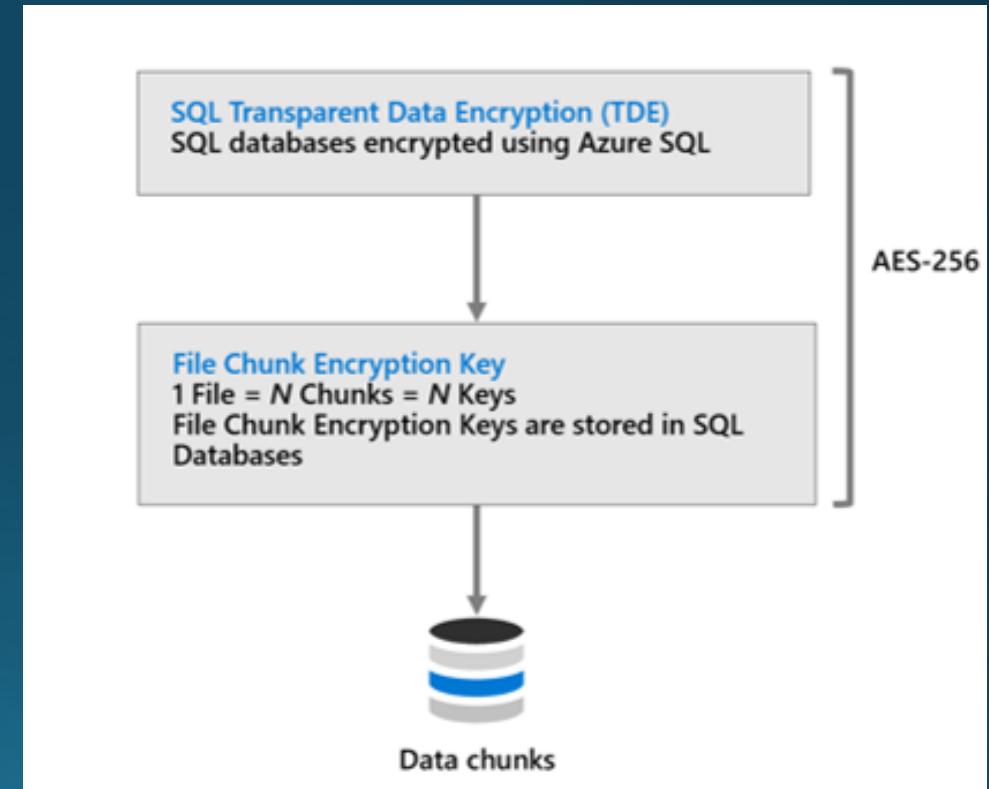
Double Key Encryption (MPIP)

Microsoft managed

Exchange Online



SharePoint Online, OneDrive



Customer key

Organization in control

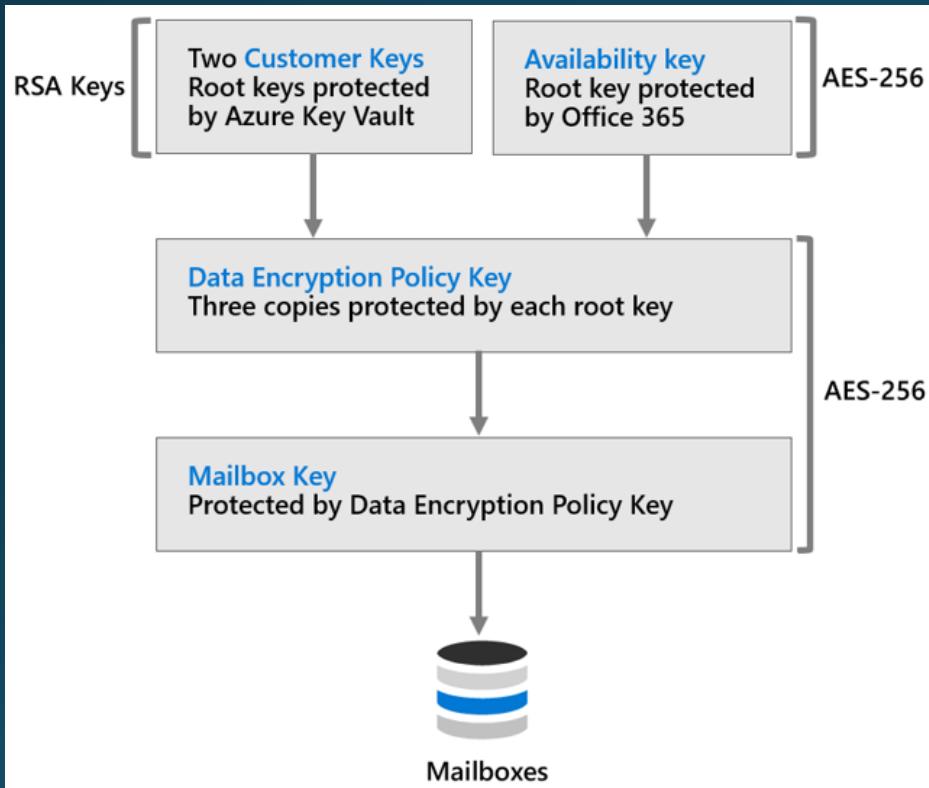
Access by Microsoft

Different DEPs, including multi-geo

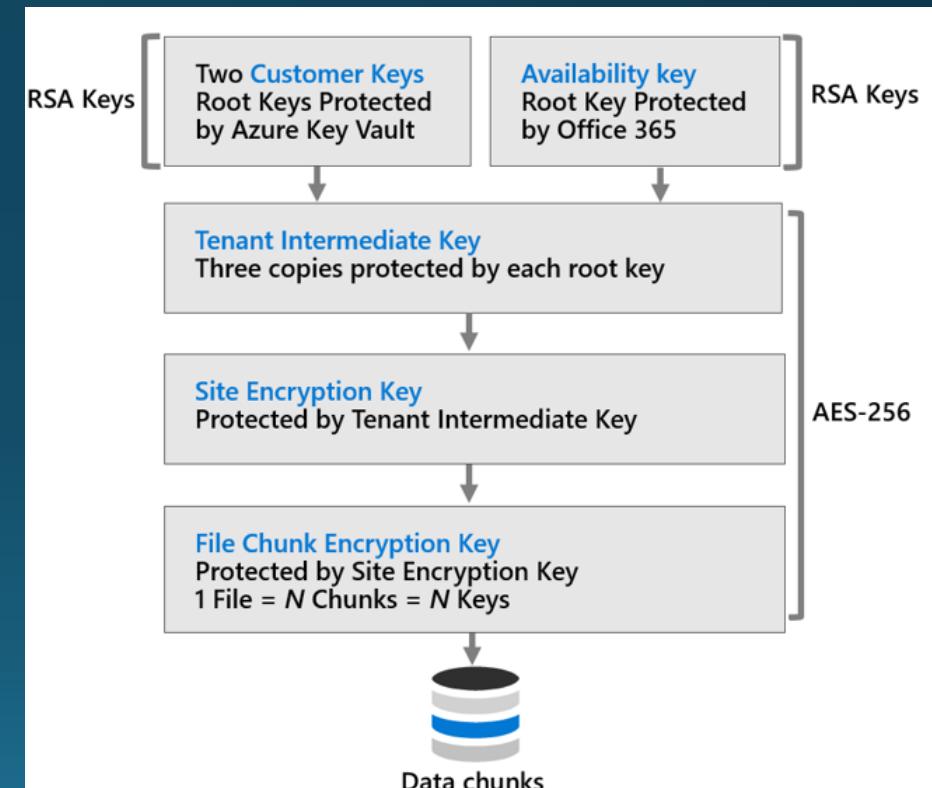
Azure Key Vault
Hardware Security Modules

Customer Key

Exchange Online

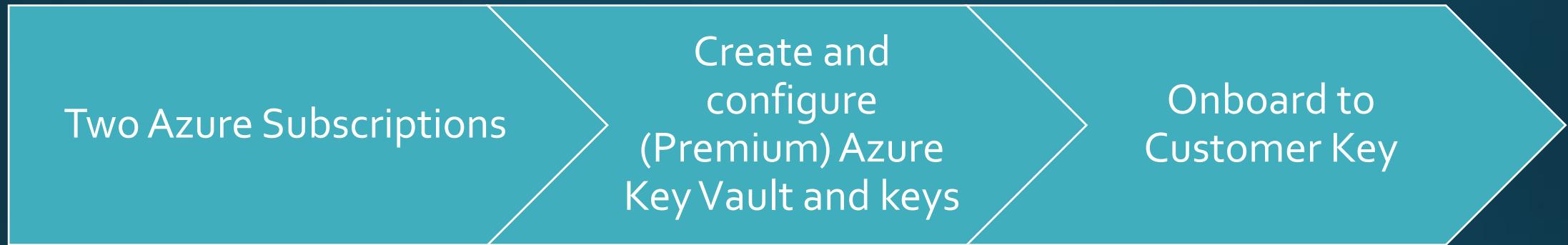


SharePoint Online, OneDrive



Customer Key per DEP

<https://learn.microsoft.com/en-us/purview/customer-key-set-up>



 **Customer Key for SharePoint and OneDrive for Business**

Enables Office 365 customers to use encryption keys with SharePoint and OneDrive for Business that the customer owns and controls.

[Request encryption key help for Sharepoint and OneDrive >](#)

 **Customer Key for Exchange**

Enables Office 365 customers to use encryption keys with Exchange Online that the customer owns and controls.

[Request encryption key help for Exchange online >](#)

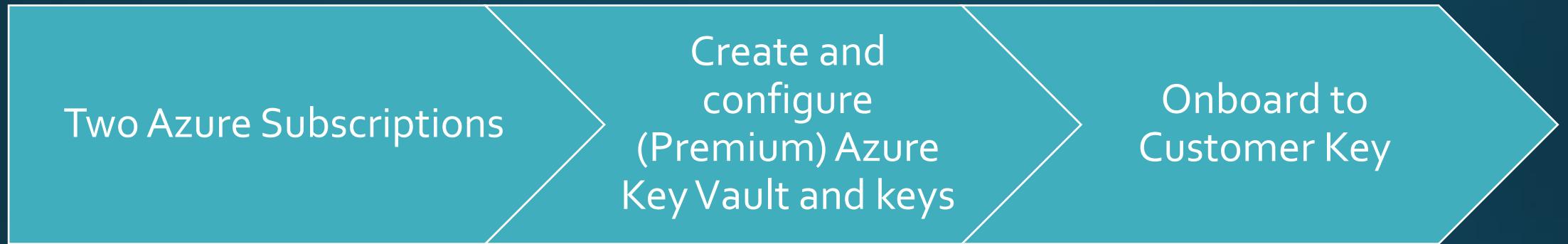
 **Customer key for Microsoft 365**

Enables Microsoft 365 customers to use their own encryption keys to protect data-at-rest for multiple Microsoft 365 workloads.

[Request help for Microsoft 365 Customer Key >](#)

Customer Key per DEP

<https://learn.microsoft.com/en-us/purview/customer-key-set-up>



Onboard using the Customer Key Onboarding Service

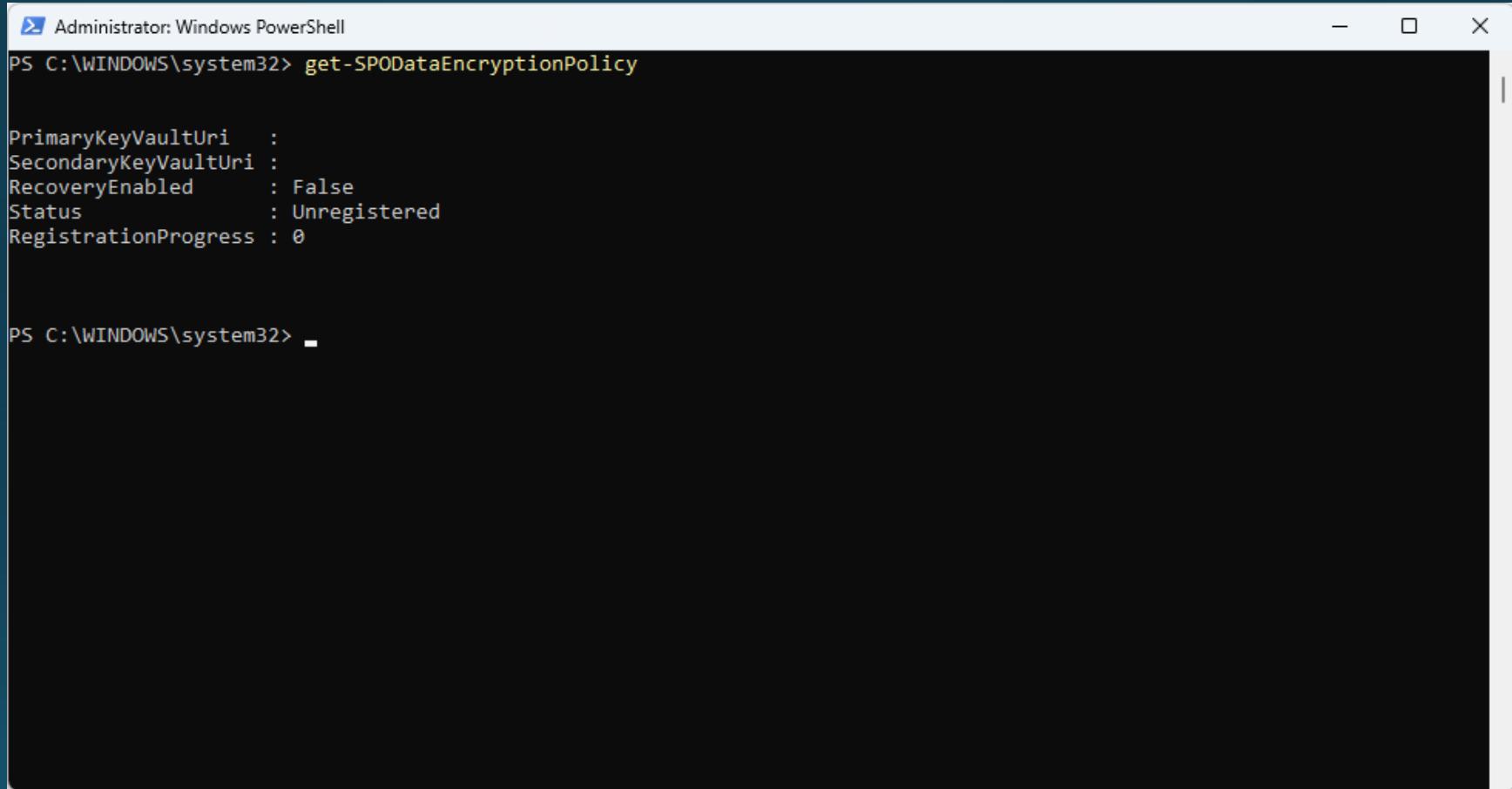
The Microsoft 365 Customer Key Onboarding Service is a service that allows you to enable Customer Key within your own tenant. This feature automatically validates the required Customer Key resources. If desired, you can validate your resources separately before proceeding with Customer Key enablement within your tenant.

ⓘ Important

This service isn't yet available for the following scenarios:

- Government tenants - see "Onboard to Customer Key for Government tenants" below.
- SharePoint and OneDrive - see "Onboard to Customer Key for SharePoint and OneDrive" below.
- Tenants using managed HSMs - see "Onboard to Customer Key using the legacy method" below.

Customer Key status



The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell". The command "get-SPODataEncryptionPolicy" is run, displaying the following properties:

```
PS C:\WINDOWS\system32> get-SPODataEncryptionPolicy

PrimaryKeyVaultUri    :
SecondaryKeyVaultUri :
RecoveryEnabled        : False
Status                 : Unregistered
RegistrationProgress   : 0

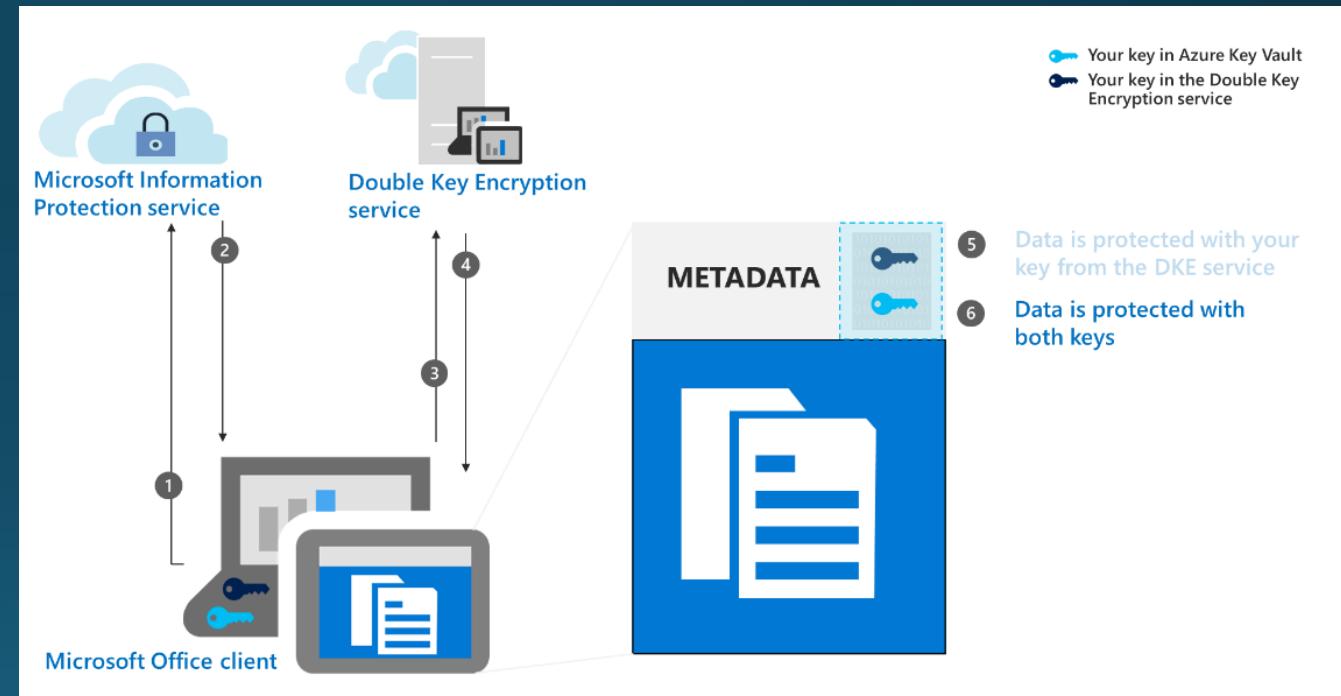
PS C:\WINDOWS\system32>
```

Double Key Encryption

Office Apps | Sensitivity labels

Tenant key and organizational key

Impairs specific functions



Double Key Encryption

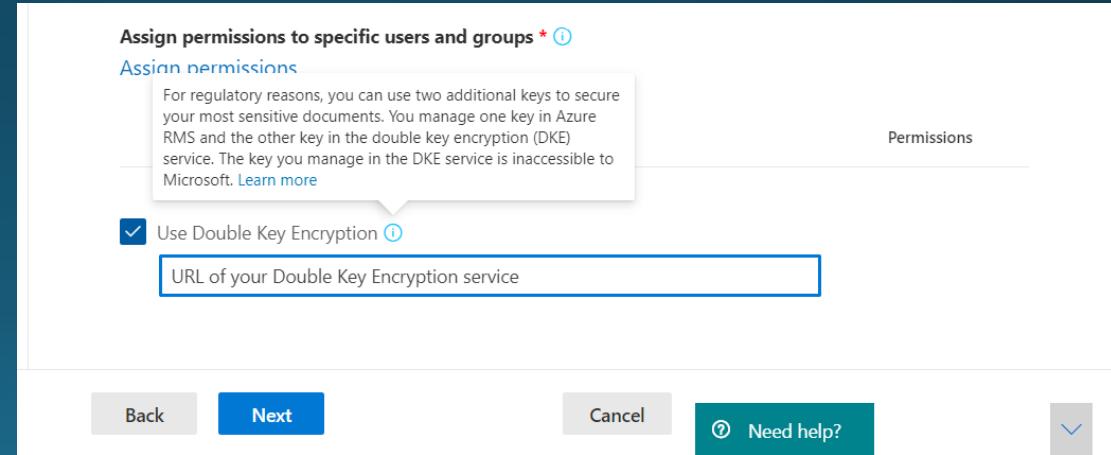
Software DKE service, GitHub

Deploy service,
publish key

Create labels with
DKE

```
    "TokenValidationParameters": {
        "ValidIssuers": [
            "https://sts.windows.net/9c99431e-b513-44be-a7d9-e7b500002d4b/"
        ]
    },
    "Logging": {
        "LogLevel": {
            "Default": "Warning"
        }
    },
    "AllowedHosts": "*",
    "JwtAudience": "https://dkeservice.contoso.com/",
    "JwtAuthorization": "https://login.windows.net/common/oauth2/authorize",
    "RoleAuthorizer": {
        "LDAPPath": ""
    },
    "TestKeys": [
        {
            "Name": "TestKey1",
            "Id": "DCE1CC21-FF9B-4424-8FF4-9914BD19A1BE",
        }
    ]
}
```

IMPORTANT! JwtAudience must match the hostname of the computer on which you installed the DKE service.





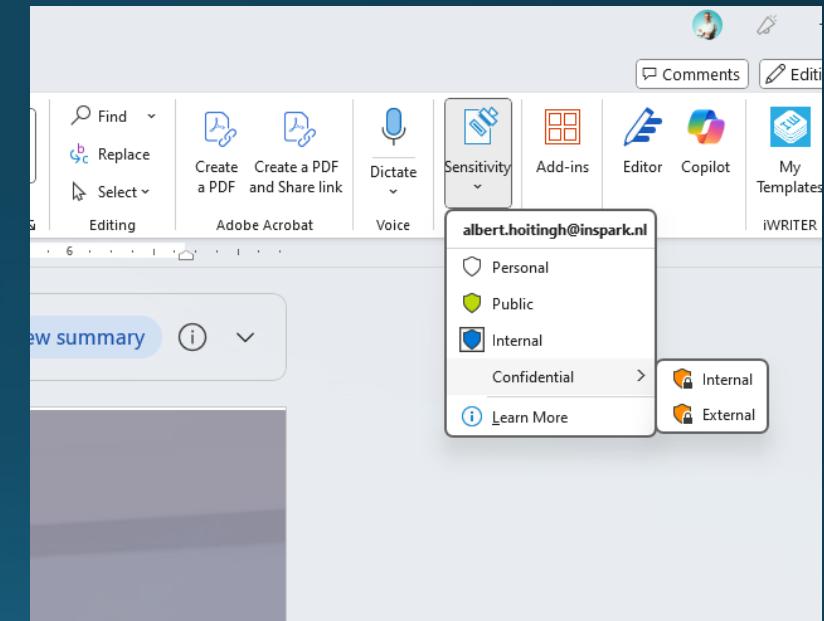
Sensitivity labels

Items and labels

Label stays with item

Encryption |
Visual markings |
Offline availability

Hierarchy is important



Encryption standards



1

Content key

Symmetric AES256-CBC
(Cypher Block Chaining)

2

Key protection

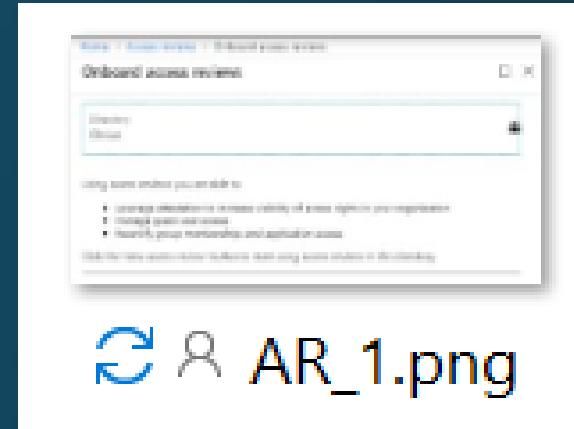
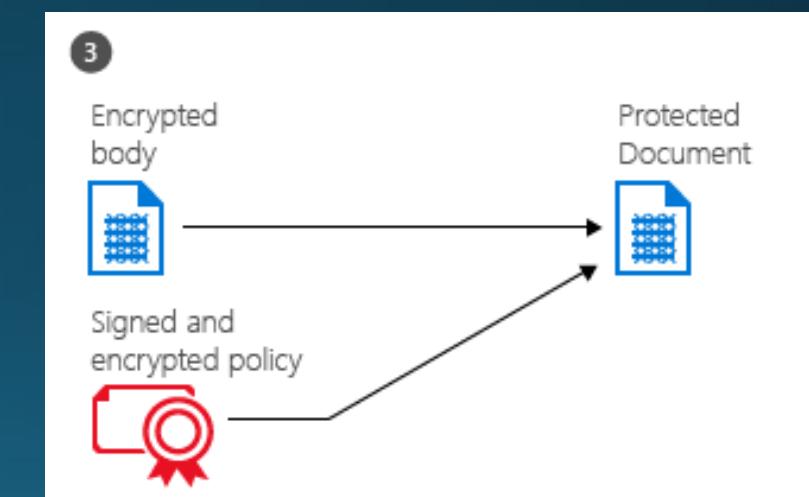
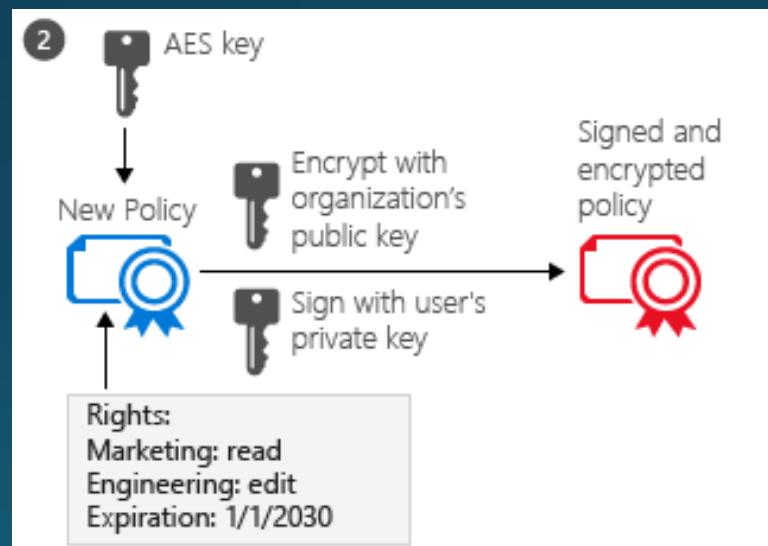
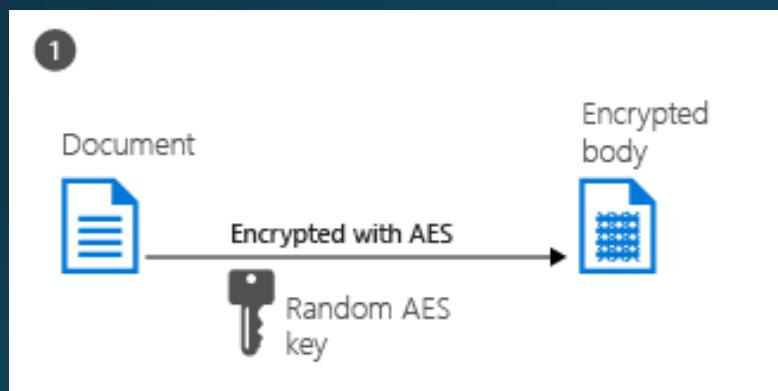
Asymmetric
RSA 2048 bit

3

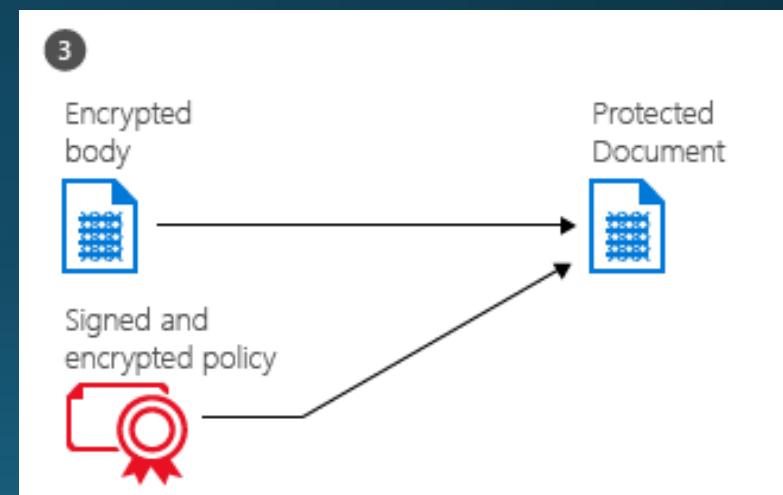
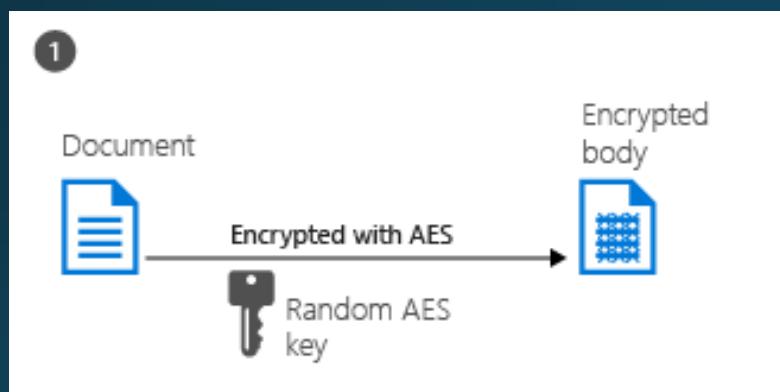
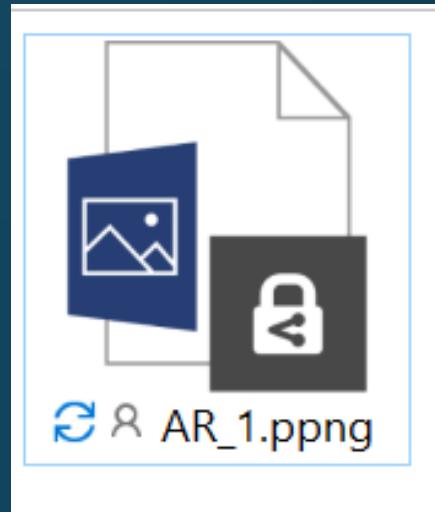
Certificate signing

SHA-256

How it works



How it works

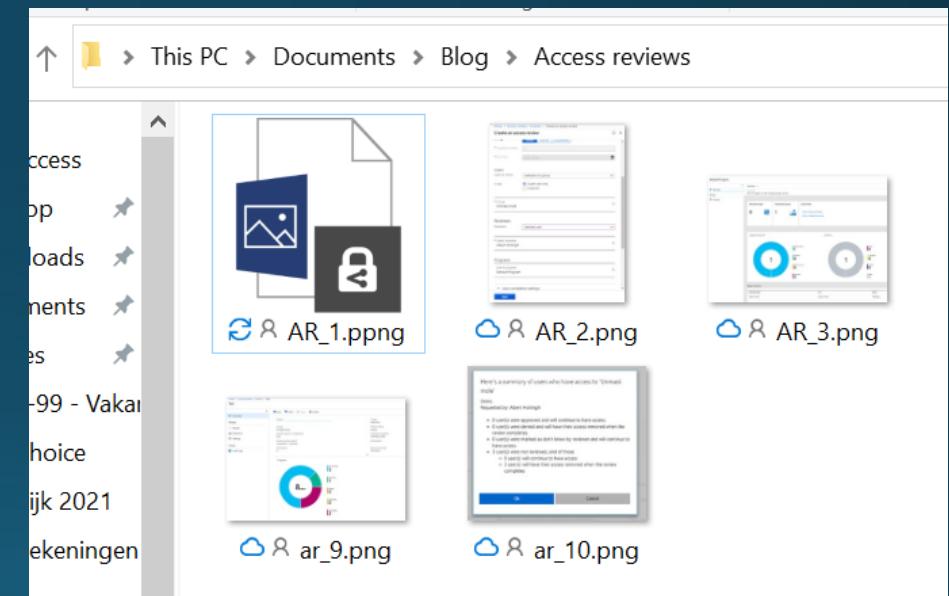


Filetypes are important

Native clients | Microsoft Edge

Microsoft Purview Information Protection Viewer client

Watch out for the file extension | some types only support classification



Identities are important

Entra ID accounts

Microsoft Live | Guest | RMS

Set-SPOTenant -
EnableAzureADB2BIntegration

RMS for individuals is a free self-service subscription for users who need to open files that have been protected by Azure Information Protection. If these users cannot be authenticated by Azure Active Directory, this free sign-up service can create an account in Azure Active Directory for a user. As a result, these users can now authenticate by using their company email address and then read the protected files on computers or mobile devices.

 Users who don't already have an Azure AD or Microsoft account can sign in without having to create an account. Each time the user signs in to your directory, they receive a passcode via email for authentication. You can also enable self-service sign-up with email one-time passcode for specific apps in your user flows.

Email one-time passcode for guests

Yes

No

Identities are important

Entra ID accounts

RMS for individuals is a free self-service subscription for users who need to open files that have been protected by Azure Information Protection. If these users cannot be authenticated by Azure Active Directory, this free sign-up service can create an account in Azure Active Directory for a user. As a result, these users can now authenticate by using their company email address and then read the protected files on computers or mobile devices.

- i** Users who don't already have an Azure AD or Microsoft account can sign in without having to create an account. Each time the user signs in to your directory, they receive a passcode via email for authentication. You can also enable self-service sign-up with email one-time passcode for specific apps in your user flows. →

Email one-time passcode for guests

Yes

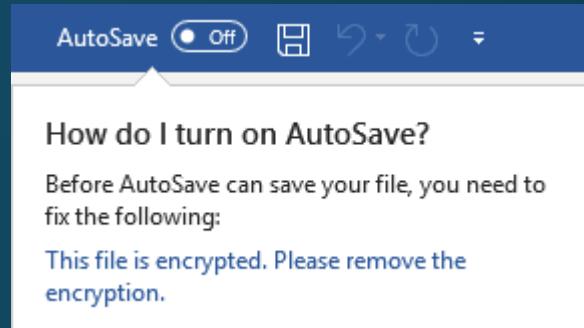
No

Consequences

Co-authoring | auto-save

eDiscovery | content search

Microsoft 365 Copilot



Settings > Co-authoring for files with sensitivity labels

Co-authoring for files with sensitivity labels

This setting allows users in your organization to co-author in Office desktop documents that are encrypted by using sensitivity labels. To support this new capability, all users must have the latest Microsoft 365 Apps for enterprise and label metadata must be upgraded for all labeled documents that aren't encrypted. [Learn more about this one-time setting](#)

Prerequisites

- Sensitivity labels must be enabled for files in OneDrive and SharePoint. If this isn't already done, we'll enable this for you when you turn on co-authoring.
- Minimum versions of apps to support the new labeling metadata.
- Latest Microsoft 365 Apps for enterprise.
- Any labeling apps or solutions you've deployed use the minimum supported version of the MIP SDK.
- Any scripts or tools you're using that read from or write to the labeling metadata for documents are updated to use the new metadata format and location.

[Learn more about these prerequisites](#)

What to expect after turning this on

- When existing labeled and unencrypted documents are opened and saved, the sensitivity label information that's currently stored as a custom property is copied and saved to a new format in a new metadata location.

Turn on co-authoring for files with sensitivity labels

When this was turned on, we also enabled sensitivity labels for files in OneDrive and SharePoint if it wasn't already enabled. [Learn more](#)

⚠️ You can't turn this setting off because this action can result in losing some labeling information. If you accept this risk and still want to turn it off, contact Microsoft Support. [Learn more](#)

[Apply](#) [Cancel](#)

Consequences

Co-authoring | auto-save

eDiscovery | content search

Microsoft 365 Copilot

eDiscovery task	Content search	eDiscovery (Standard)	eDiscovery (Premium)
Search for content in encrypted files in sites and email attachments ¹	No	No	Yes
Preview encrypted files attached to email	Yes	Yes	Yes
Preview encrypted documents in SharePoint and OneDrive	No	No	Yes
Review encrypted files in a review set	N/A	N/A	Yes
Export encrypted files attached to email	Yes	Yes	Yes
Export encrypted documents in SharePoint and OneDrive	No	No	Yes

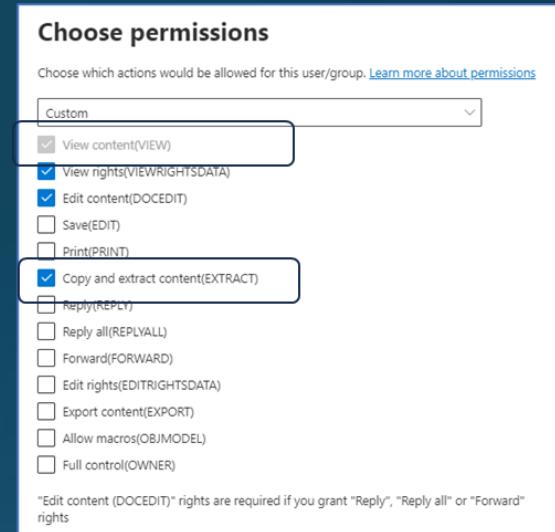
Item type	Task	eDiscovery (Standard)	eDiscovery (Premium)
Encrypted email	Search	Yes	Yes
Encrypted email	Decryption to .pst	No	Yes
Encrypted email	Decryption to file	Yes	Yes
Encrypted mail and attachment	Search	No	Yes (with Advanced indexing) ¹
Encrypted mail and attachment	Decryption to .pst	No	Yes
Encrypted mail and attachment	Decryption to file	No	Yes
File in SharePoint with MIP label	Search	No	Yes
File in SharePoint with MIP label	Decryption	No	Yes
File in SharePoint with other encryption ²	Search, Decryption	No	No

Consequences

Co-authoring | auto-save

eDiscovery | content search

Microsoft 365 Copilot



Edit sensitivity label

 Label details Scope Items Access control Content marking Auto-labeling for files and emails Groups & sites Schematized data assets (preview) Finish

Access control

Use encryption capabilities to control who can access labeled items. Depending on the scope you specified, items can include emails, Office, Fabric and Power BI files, and meeting invites. [Learn more about access control settings](#)

Remove access control settings if already applied to items

Configure access control settings

Assign permissions now or let users decide?

Assign permissions now

The settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires [\(i\)](#)

Never

Allow offline access [\(i\)](#)

Always

Assign permissions to specific users and groups * [\(i\)](#)

Assign permissions

1 item

Users and groups	Permissions	Edit	Delete
5003084.onmicrosoft.com	Co-Author		

Use Double Key Encryption [\(i\)](#)

Assign permissions now or let users decide?

Let users assign permissions when they apply the label

(i) The labeling behavior for these settings varies depending on which operating system platform is used to apply the label. [Learn more](#)

In Outlook, enforce one of the following restrictions

Do Not Forward (i)

Encrypt-Only (i)

In Word, PowerPoint, and Excel, prompt users to specify permissions (i)

Use Double Key Encryption (i)

Permissions

Specify who can do what (i)

Viewer

The user can view. They can't edit, print, copy content, or change/remove protection.

Restricted Editor

The user can view and edit. But they can't print, copy content, or change/remove protection.

Editor

The user can view, edit, print and copy content. But they can't change/remove protection.

Owner

The user can do anything with the document, including remove protection.



albert.hoitingh@inspark.nl

> More Options (i)

Apply

Cancel

Assign permissions

Only the users or groups you choose will be assigned permissions to use the content that has this label applied. You can choose from existing permissions (such as Co-Owner, Co-Author, and Reviewer) or customize them to meet your needs.

+ Add all users and groups in your organization

+ Add any authenticated users ⓘ

+ Add users or groups

+ Add specific email addresses or domains ⓘ

0 items

Permissions assigned to

Delete

No data available

Choose permissions

Co-Author

View content, View rights, Edit content, Save, Print, Copy and extract content, Reply, Reply all, Forward, Allow macros

Choose permissions

Choose which actions would be allowed for this user/group. [Learn more about permissions](#)

Viewer

Owner

Editor

Restricted Editor

Viewer

Custom

Copy and extract content(EXTRACT)

Reply(REPLY)

Reply all(REPLYALL)

Forward(FORWARD)

Edit rights(EDITRIGHTSDATA)

Export content(EXPORT)

Allow macros(OBJMODEL)

Full control(OWNER)



Assign permissions

Only the users or groups you choose will be assigned permissions to use the content that has this label applied. You can choose from existing permissions (such as Co-Owner, Co-Author, and Reviewer) or customize them to meet your needs.

+ Add all users and groups in your organization

+ Add any authenticated users ⓘ

+ Add users or groups

+ Add specific email addresses or domains ⓘ

0 items

Permissions assigned to

Delete

No data available

Choose permissions

Co-Author

View content, View rights, Edit content, Save, Print, Copy and extract content, Reply, Reply all, Forward, Allow macros

Choose permissions

Choose which actions would be allowed for this user/group. [Learn more about permissions](#)

Co-Owner

Co-Owner

Co-Author

Reviewer

Viewer

Custom

Copy and extract content(EXTRACT)

Reply(REPLY)

Reply all(REPLYALL)

Forward(FORWARD)

Edit rights(EDITRIGHTSDATA)

Export content(EXPORT)

Allow macros(OBJMODEL)

Full control(OWNER)





Microsoft Purview Message Encryption

Secure e-mail in Microsoft 365

The screenshot illustrates the Microsoft 365 Mail interface with two overlapping context menus demonstrating security features.

Top Context Menu (Left):

- Shows standard mail options: **Show Cc** (checked), **Show From**, **Request delivery receipt**.
- Contains a "Send" button and a "Send" dropdown.
- Has "To" and "Cc" input fields.
- An "Options" tab is selected.
- A "Set permissions on this item" section includes:
 - Encrypt**
 - Do Not Forward**
 - No permission set** (indicated by a green checkmark)

Bottom Context Menu (Right):

- Shows standard mail options: **Show Cc** (checked), **Show From**, **Request delivery receipt**, **Request read receipt**, **Disallow**.
- Contains a "Send" button and a "Send" dropdown.
- Has "To" and "Cc" input fields.
- An "Options" tab is selected.
- A "Set permissions on this item" section includes:
 - Personal** (blue shield icon)
 - Public** (green shield icon)
 - Confidential** (blue shield icon)
 - Highly Confidential** (blue shield icon)
 - Geheim** (blue shield icon)
 - Board meetings - confidential** (red shield icon)
- A sidebar lists additional protection levels:
 - All Employees
 - Anyone (not protected)
 - Set your own protection
 - Medical privacy information
 - Business meeting - not E2EE

Microsoft Purview Message Encryption



1

Any recipient and email client



2

Secure web-portal



3

Do-not-forward
Encrypt only

Advanced message encryption

Revocation and expiration

Microsoft 365

Mail rules using sensitive
information types

E5 -
Information Protection
and Governance

E5 -
Compliance

E5

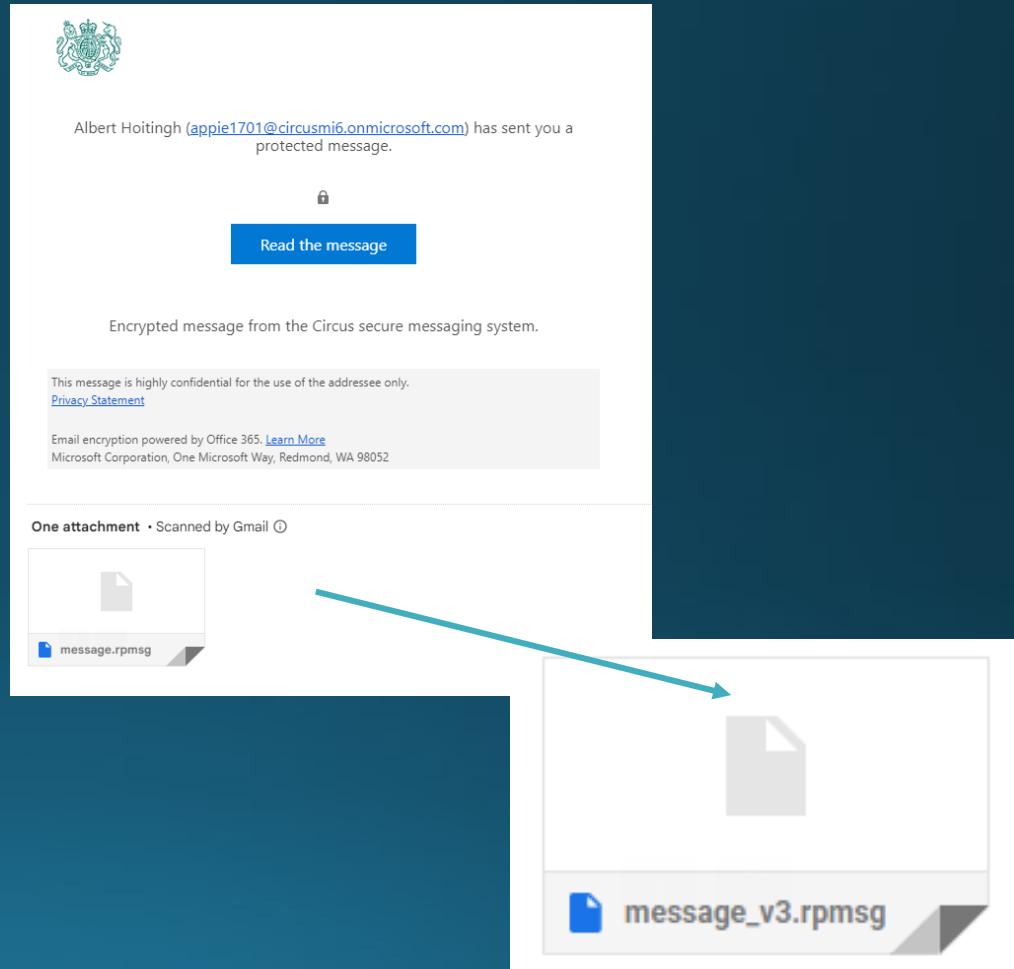
Encapsulated e-mail message

.pmsg file

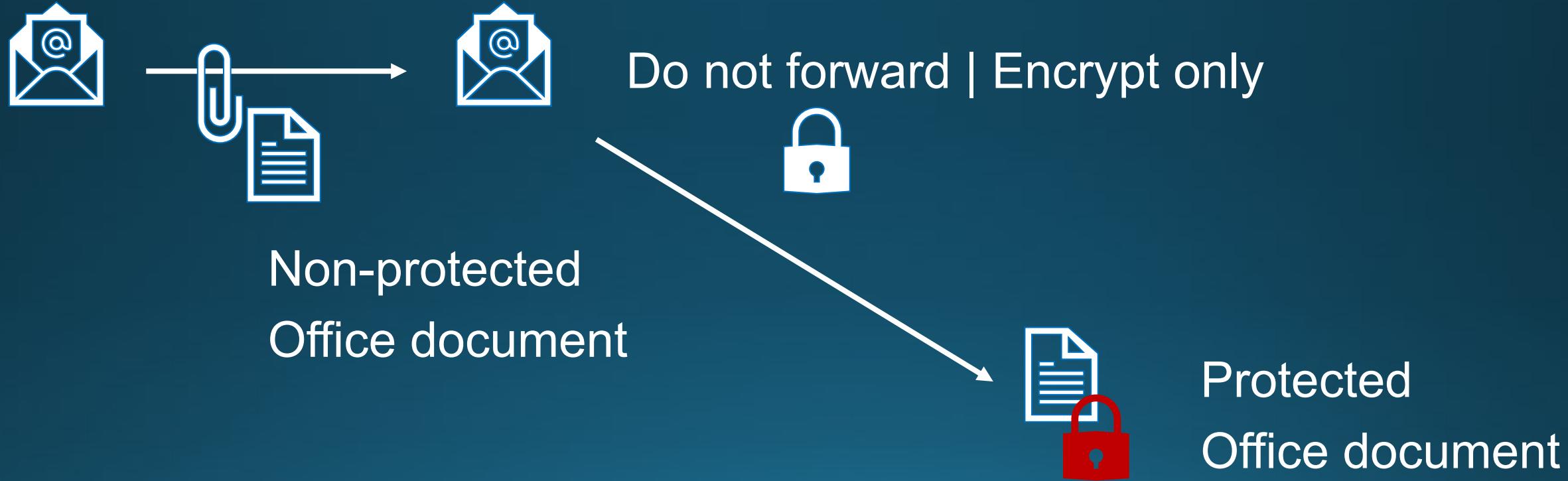
Outlook: opens natively

Secure web-portal

MPIP viewer does not work



E-mail attachments



Mind the Entra ID account

Set-IRMConfiguration - DecryptAttachmentForEncryptOnly <\$true|\$false>



Run-through Message Encryption

Send Attach Sensitivity Discard ...

Do Not Forward: Recipients can't forward, print, or copy content. [Remove encryption](#)

To Albert Hoitingh <albert.hoitingh@gmail.com> albert.hoitingh@inspark.nl

Cc

Add a subject

Albert Hoitingh.docx 12 KB

Hi there,

This is send using Do-not-forward.
Both to an Azure AD account and Gmail account.
Let's see.....

Albert



Albert Hoitingh (appie1701@circusmi6.onmicrosoft.com) has sent you a protected message.

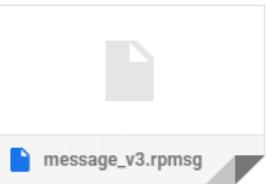


[Read the message](#)

Encrypted message from the Circus secure messaging system.

This message is highly confidential for the use of the addressee only.
[Privacy Statement](#)

Email encryption powered by Office 365. [Learn More](#)
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052



appie1701@circusmi6.onmicrosoft.com has sent you a protected message



[Sign in to view the message](#)

[Sign in with Google](#)

[Sign in with a One-time passcode](#)

[Need Help?](#)

[Privacy Statement](#)



Demo Office 365 Message Encryption

[Download](#)

Word

Find Help Give Feedback to Microsoft Terms of Use

Do Not Forward Recipients can't forward, print, or copy content.

Albert Hoitingh
Bieremalaan 67
2497 AX DEN HAAG

Hallo daar,

Dit is een document.
Met een fysiek adres en naam erin.
En een ip-adres: 127.0.0.1

168.158.21.25

Page 1 of 1

100% Give Feedback to Microsoft

This message is highly confidential for the use of the addressee only.

Albert Hoitingh

[Hide email](#)

Demo Office 365 Message Encryption

AH Albert Hoitingh
<appie1701@circusmi6.onmicrosoft.com>

Today, 9:28 AM
Appie <albert.hoitingh@gmail.com>; Albert H ✉

Albert Hoitingh.docx
59 KB

Hi there,

This is send using Do-not-forward.
Both to an Azure AD account and Gmail account.
Let's see.....

Albert

  Albert Hoitingh	Demo Office 365 Message ... Thu 10-Feb-22... 16...
 Microsoft 365 Defender Customer Connec... Join Us! M365 Defender C... Thu 10-Feb-22... 18...	
▼ Yesterday	

 This message with restricted permission cannot be viewed in the reading pane until you verify your credentials. Open the item to read its contents and verify your credentials.

Demo Office 365 Message Encryption



Albert Hoitingh <appie1701@circusmi6.onmicrosoft.com>

To Appie; Albert Hoitingh

i Do Not Forward - Recipients can't forward, print, or copy content.

Permission granted by: appie1701@circusmi6.onmicrosoft.com

If there are problems with how this message is displayed, click [here](#) to view it in a web browser.



Albert Hoitingh.docx

59 KB



Hi there,

This is send using Do-not-forward.

Both to an Azure AD account and Gmail account.

Let's see.....

Albert

Do Not Forward: Recipients can't forward, print, or copy content. [Remove encryption](#)

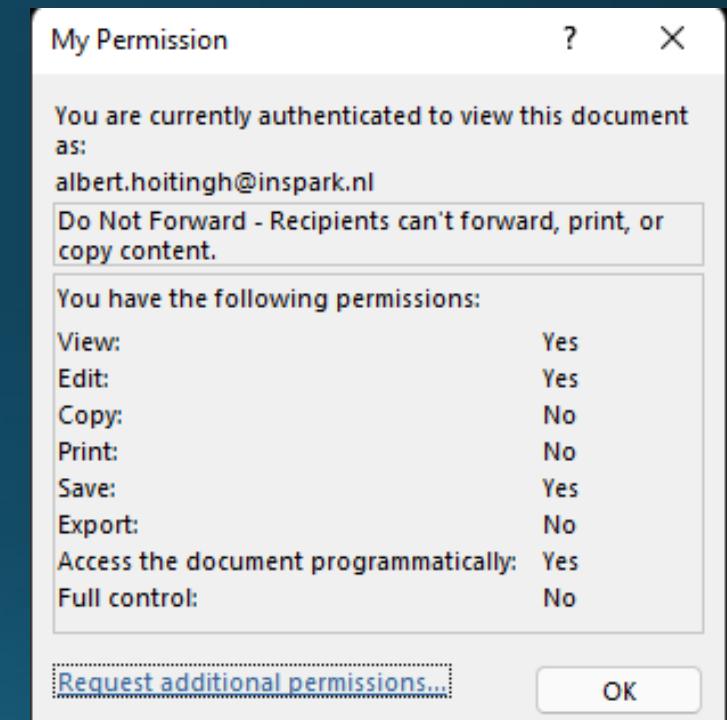
To Albert Hoitingh <albert.hoitingh@gmail.com> X albert.hoitingh@inspark.nl X

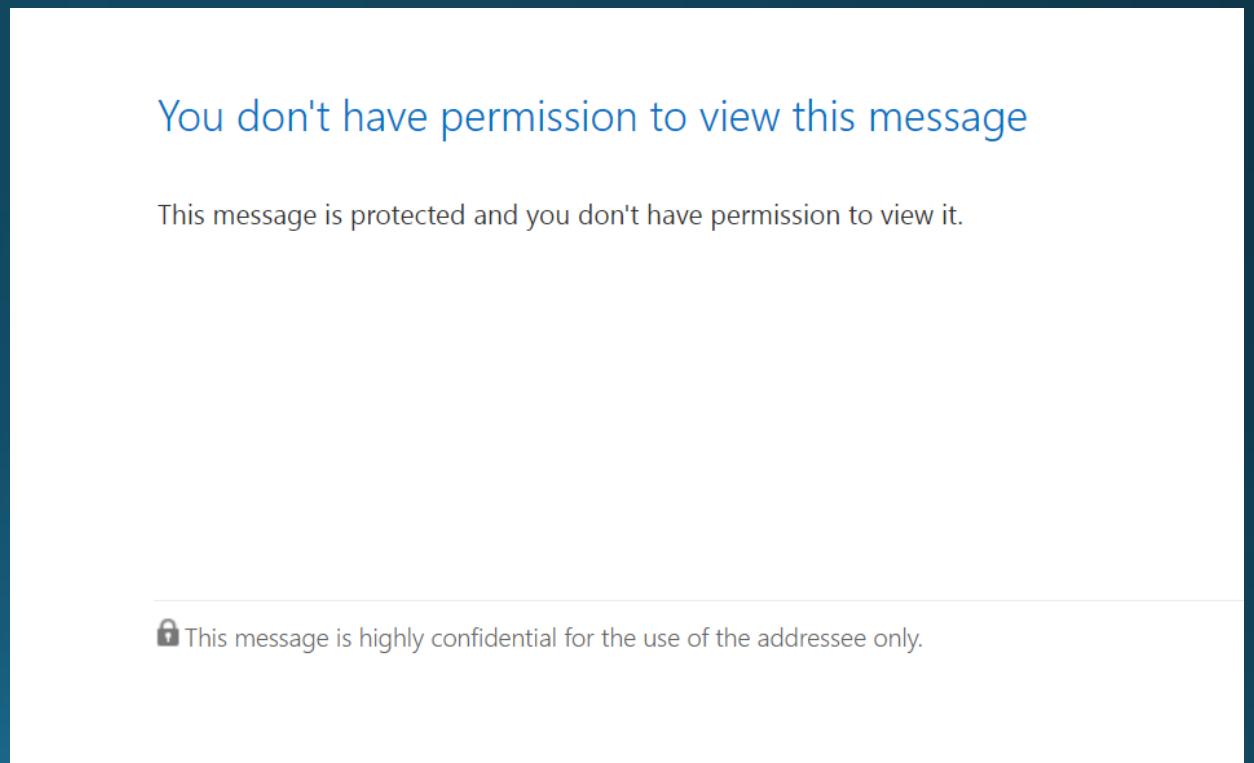
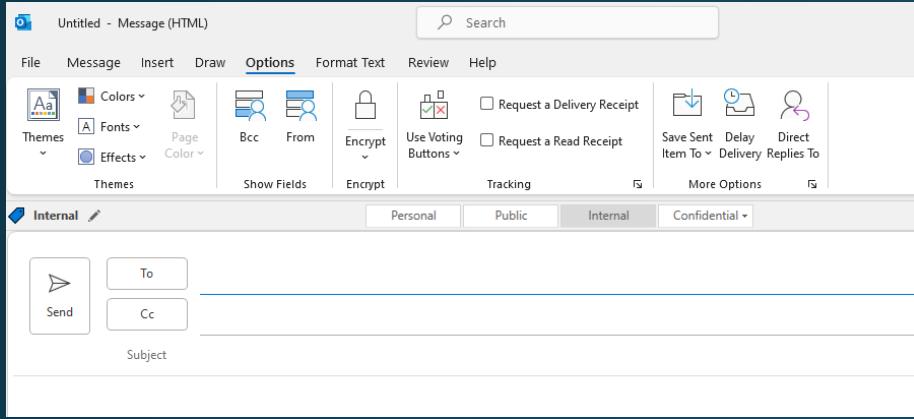
Protect with custom permissions

Select permissions

Select users, groups, or organizations

Expire access







Things to think about

Tips and tricks

Sharing encrypted files

Decrypt documents from SPO: Unlock-SensitivityLabelEncryptedFile

Guaranteed SharePoint Permissions

Older metadata model (MPIP_)

eDiscovery (Premium)

Super User role

Encrypted/Signed PDFs



Work finished

Failed: Azure Information Protection doesn't support labeling for the current file format. The file might be an old Office format.

What about migrating?

Current tenant-to-tenant workload migration capabilities

Service	Can migrate	Notes
Microsoft 365 Apps (Office 365 ProPlus)	Yes	See Reset Microsoft 365 apps for enterprise activation state .
Exchange mailboxes	Yes	Microsoft Consulting Services (MCS) and/or third-party tool
Exchange public folders	Yes	MCS and/or third-party tool
SharePoint sites	Yes	MCS and/or third-party tool
OneDrive folders	Yes	MCS and/or third-party tool
Office 365 groups	Yes	MCS and/or third-party tool
Teams	Partial	Content migration requires a third-party tool and scripts to recreate the Teams structure and permissions.
Yammer	Partial	Limited scenarios supported – requires a service ticket with Microsoft Support.
Azure Information Protection	Partial	Limited scenarios supported – requires a service ticket with Microsoft Support. Labels cannot be migrated across tenants.

<https://learn.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-tenant-to-tenant-migrations?view=o365-worldwide>

Dank jullie voor de aandacht!
Microsoft 365 en
encryptie

<https://learn.microsoft.com/en-us/purview/encryption>

