17 December 2024

Microsoft 365 en encryptie

Albert Hoitingh

Principal consultant @ InSpark

Microsoft® Most Valuable Professional

CISSP® Certified Information Systems Security Professional

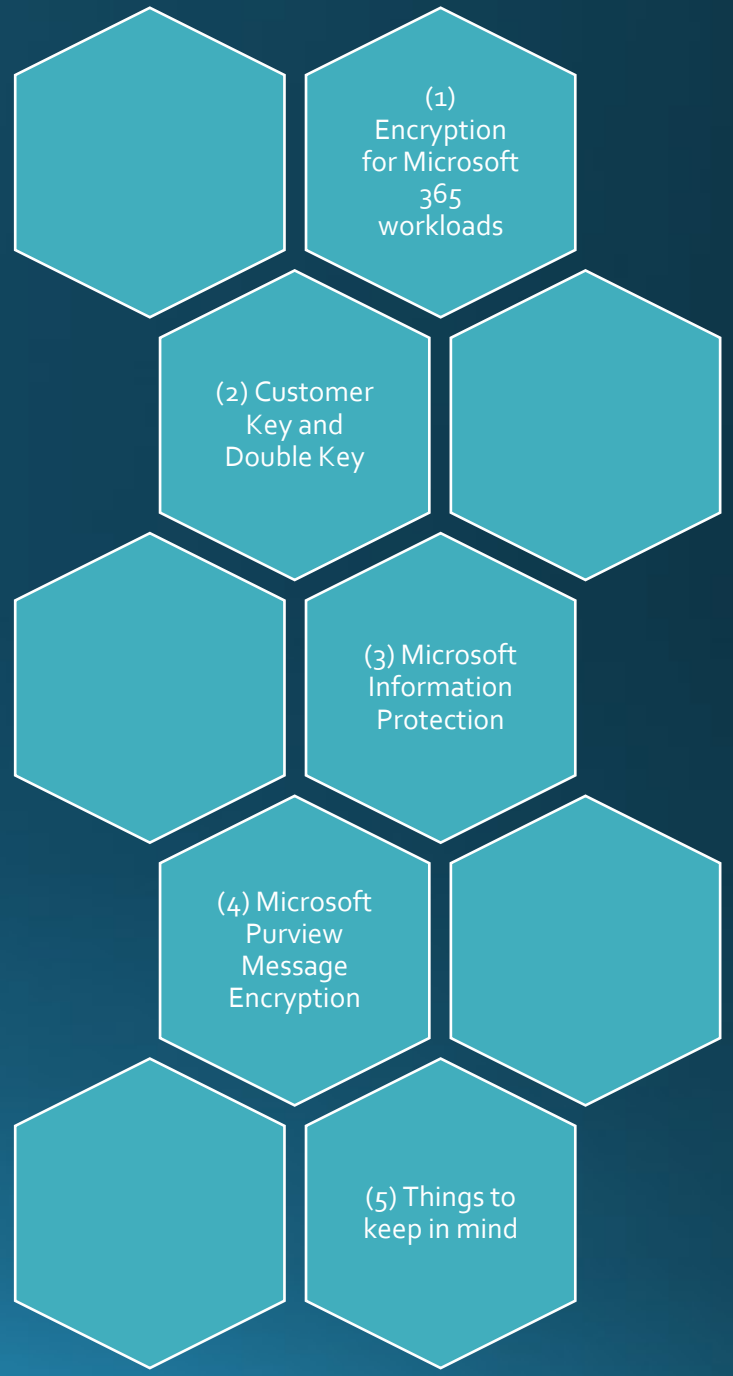
Microsoft 365 | Security

@Alberthoitingh

https://linkedin.com/in/appieh

https://alberthoitingh.com

Today's agenda




Encryption in Microsoft 365 and Purview

Different scopes

1

At rest

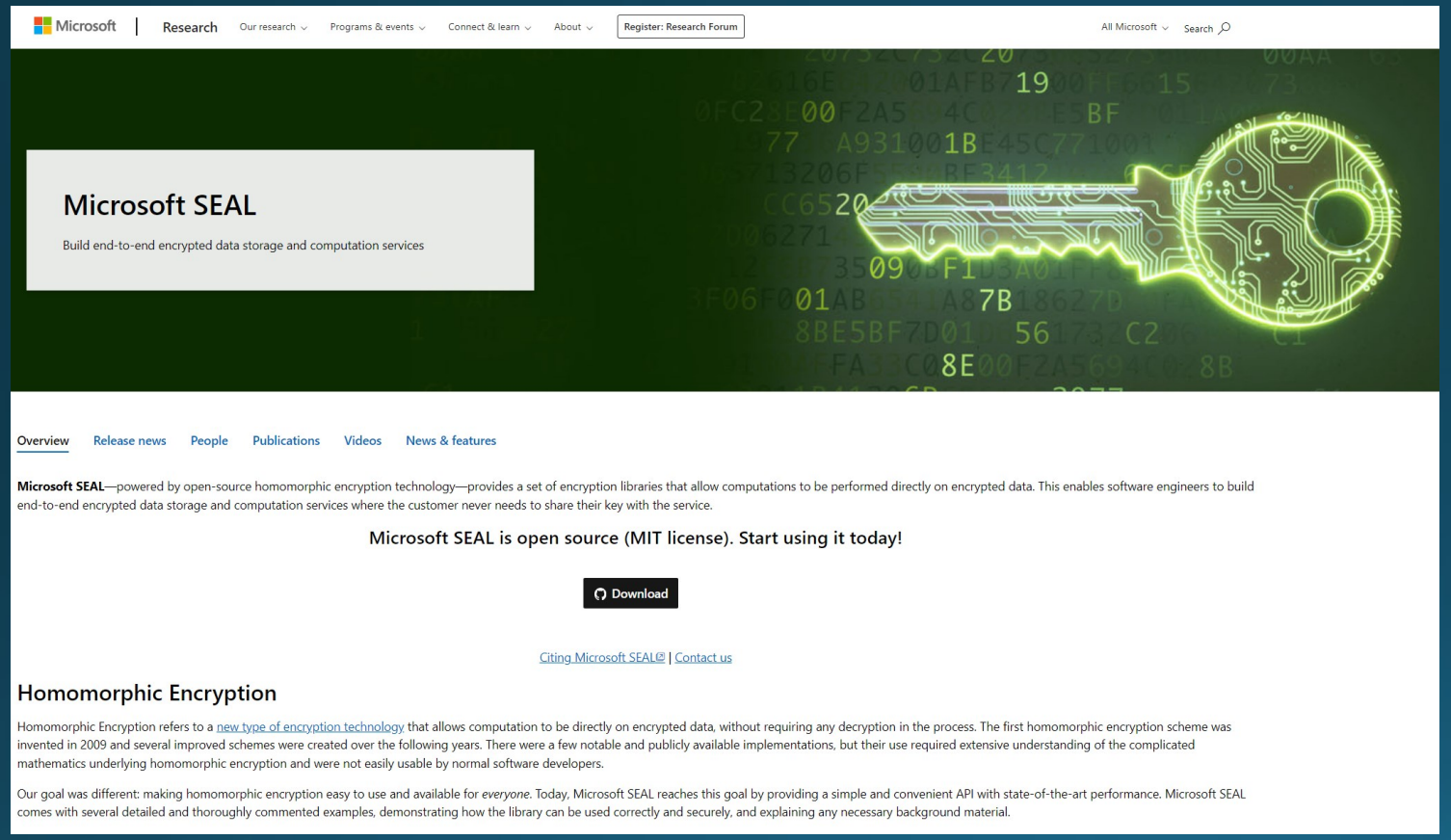
2

In transit

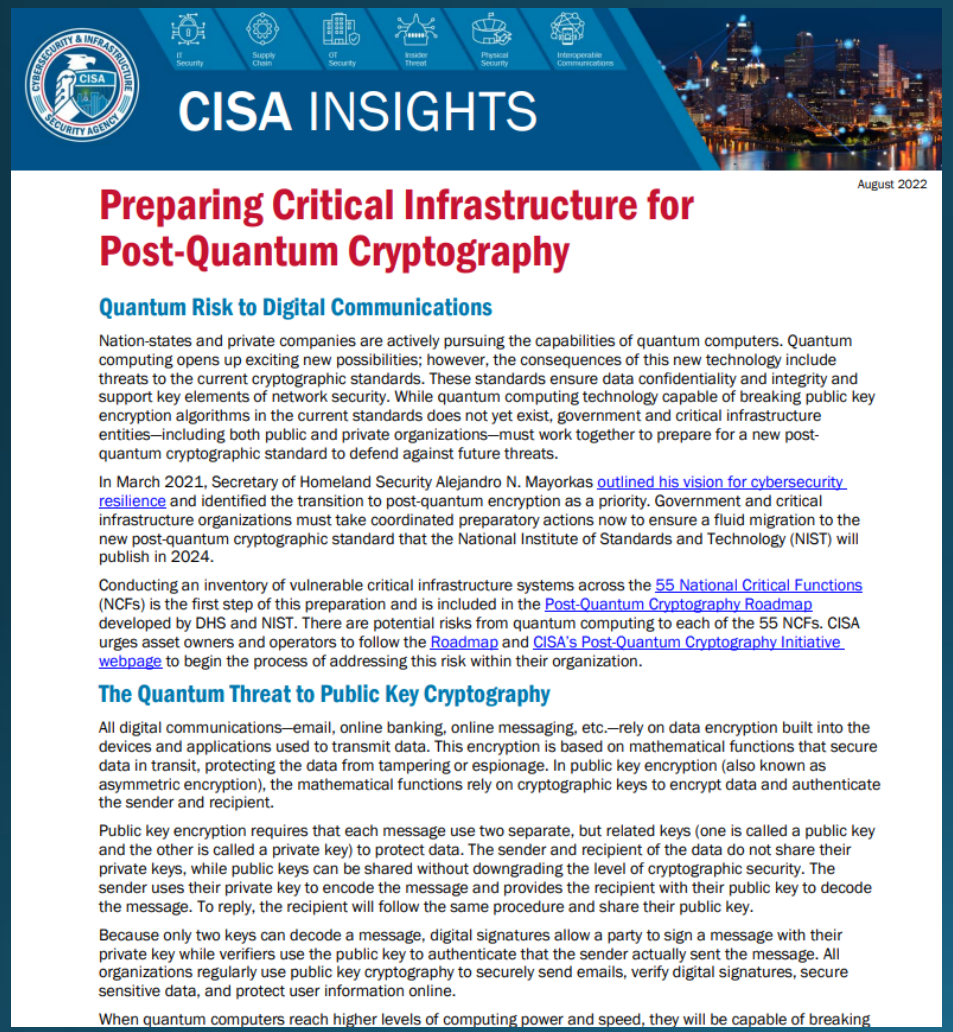
3

Specific functions

Short side note…



Short side note…



CISA INSIGHTS

August 2022

Preparing Critical Infrastructure for Post-Quantum Cryptography

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

Twitter Facebook LinkedIn Credit Eligible Get Permission

Licensing considerations

1

Basic functions

2

eDiscovery (Premium)

3

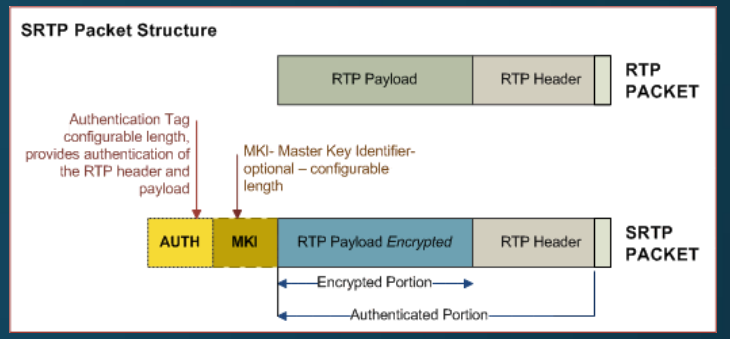
Customer Key
Double Key Encryption
Advanced Managed Encryption

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

2

3

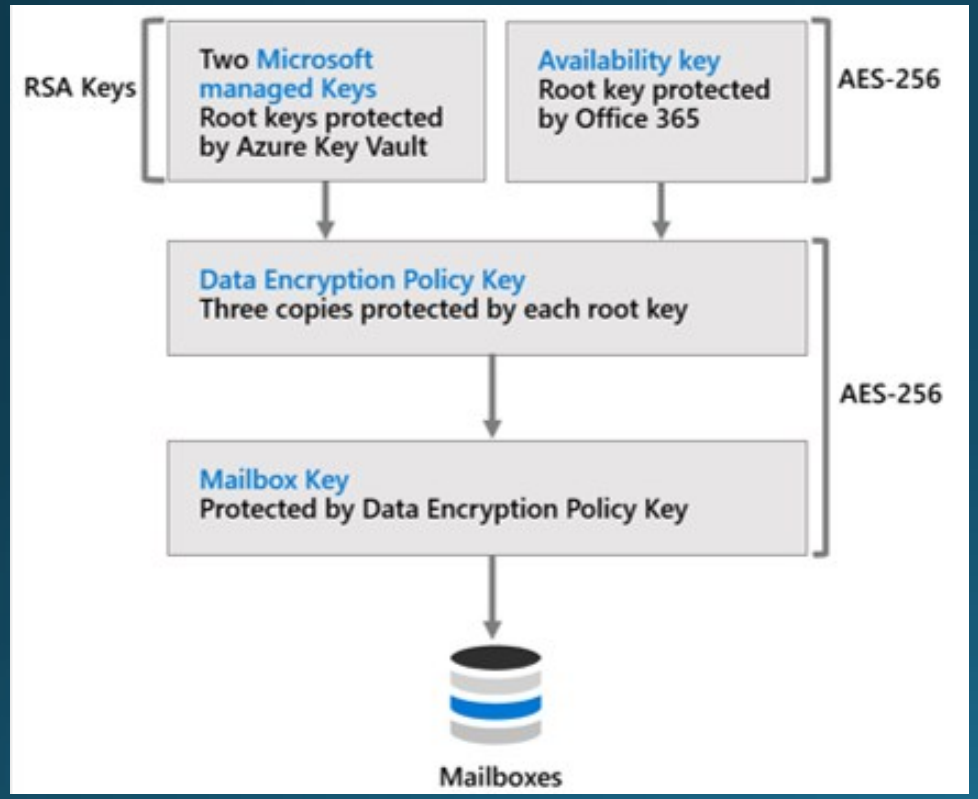
Microsoft managed

Customer Key

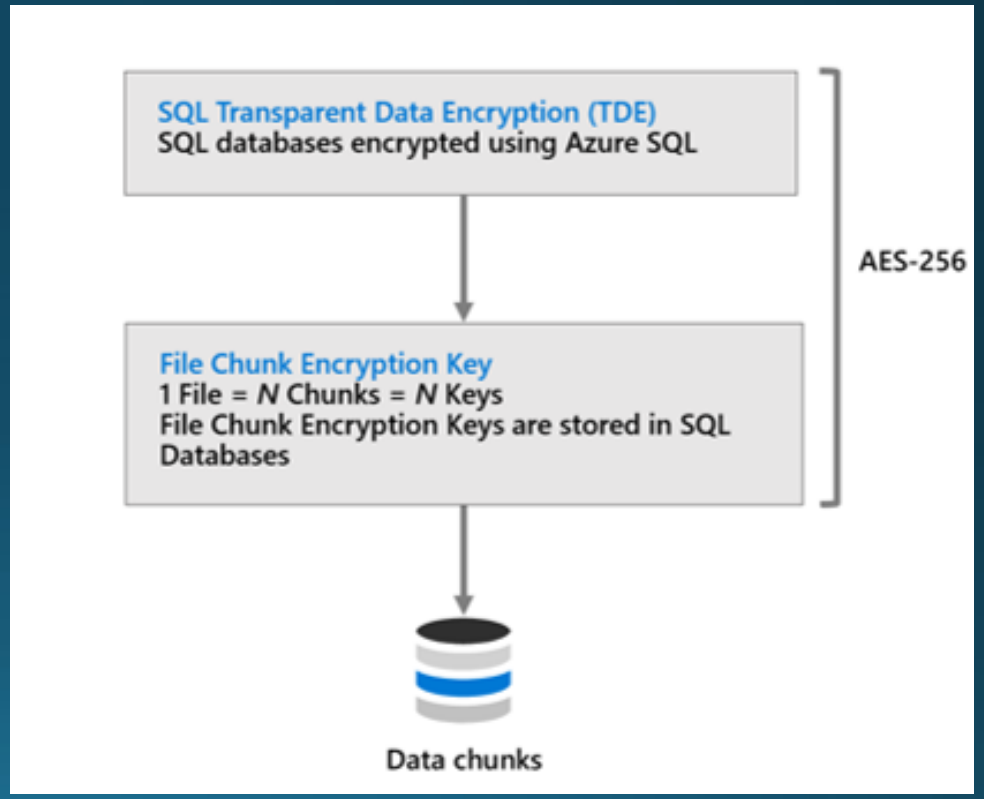
Double Key Encryption (MPIP)

Microsoft managed

Exchange Online



SharePoint Online, OneDrive



Customer key

Organization in control

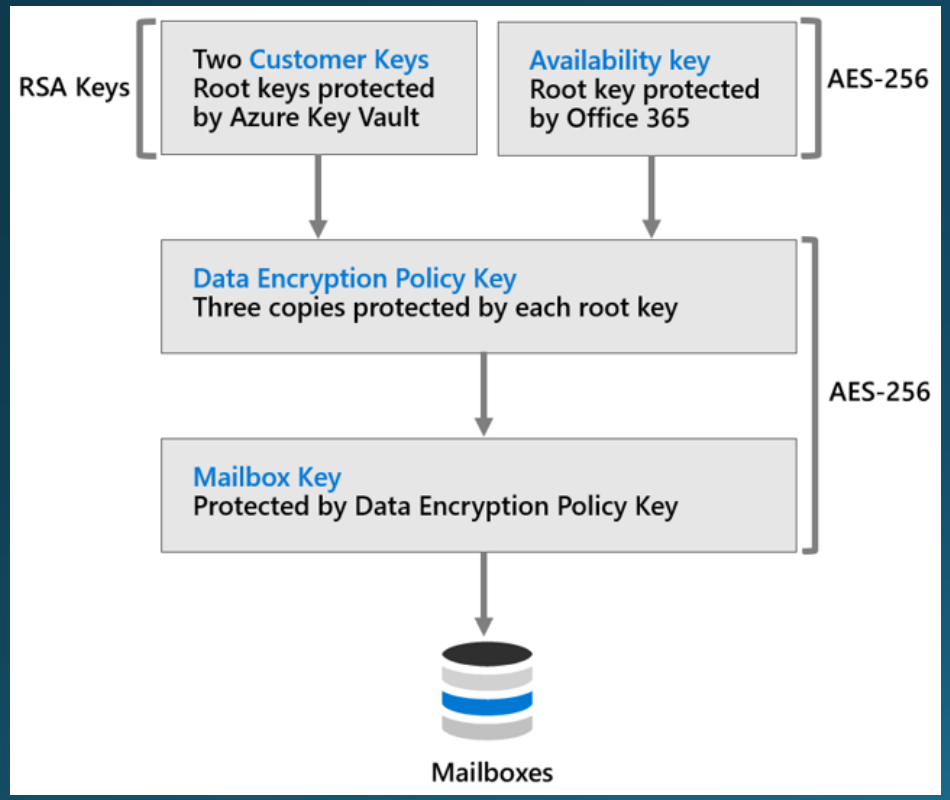
Access by Microsoft

Different DEPs, including multi-geo

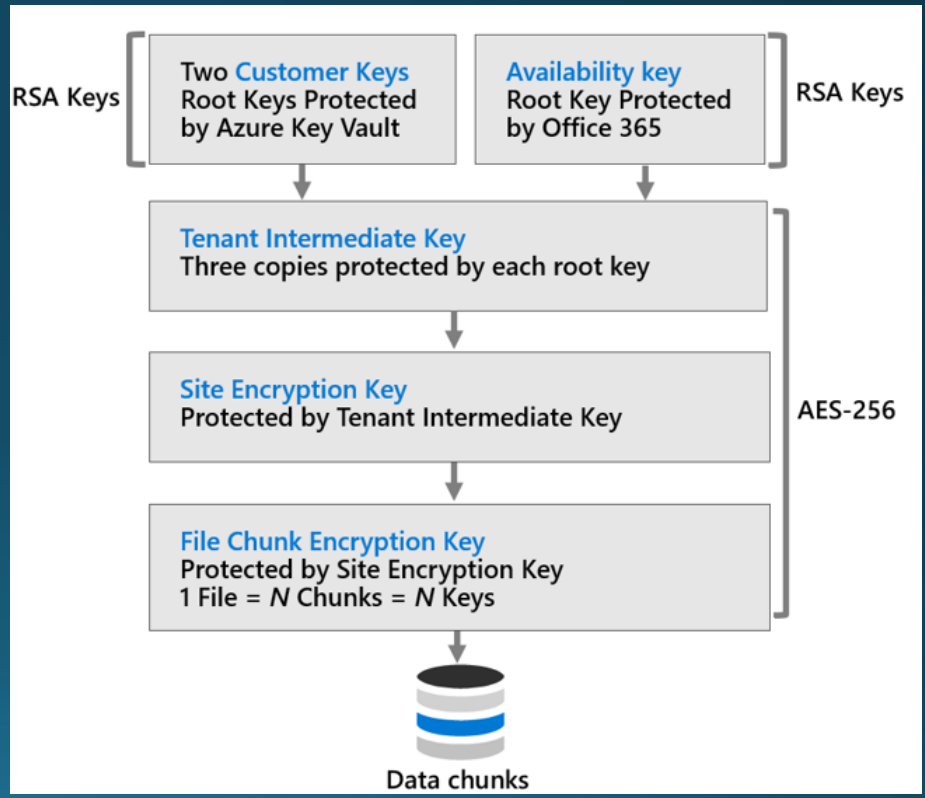
Azure Key Vault
Hardware Security Modules

Customer Key

Exchange Online



SharePoint Online, OneDrive



Customer Key per DEP

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

Two Azure Subscriptions

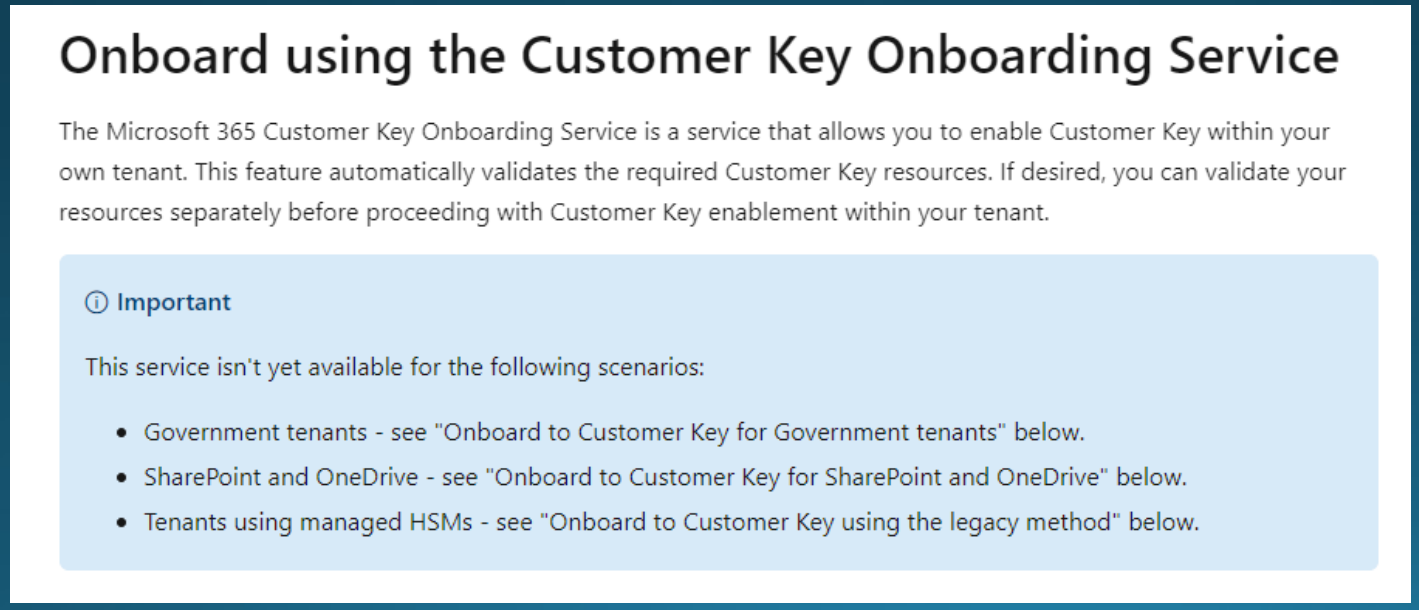
Create and configure (Premium) Azure Key Vault and keys

Onboard to Customer Key

Customer Key per DEP

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

Two Azure Subscriptions → Create and configure (Premium) Azure Key Vault and keys → Onboard to Customer Key



Onboard using the Customer Key Onboarding Service

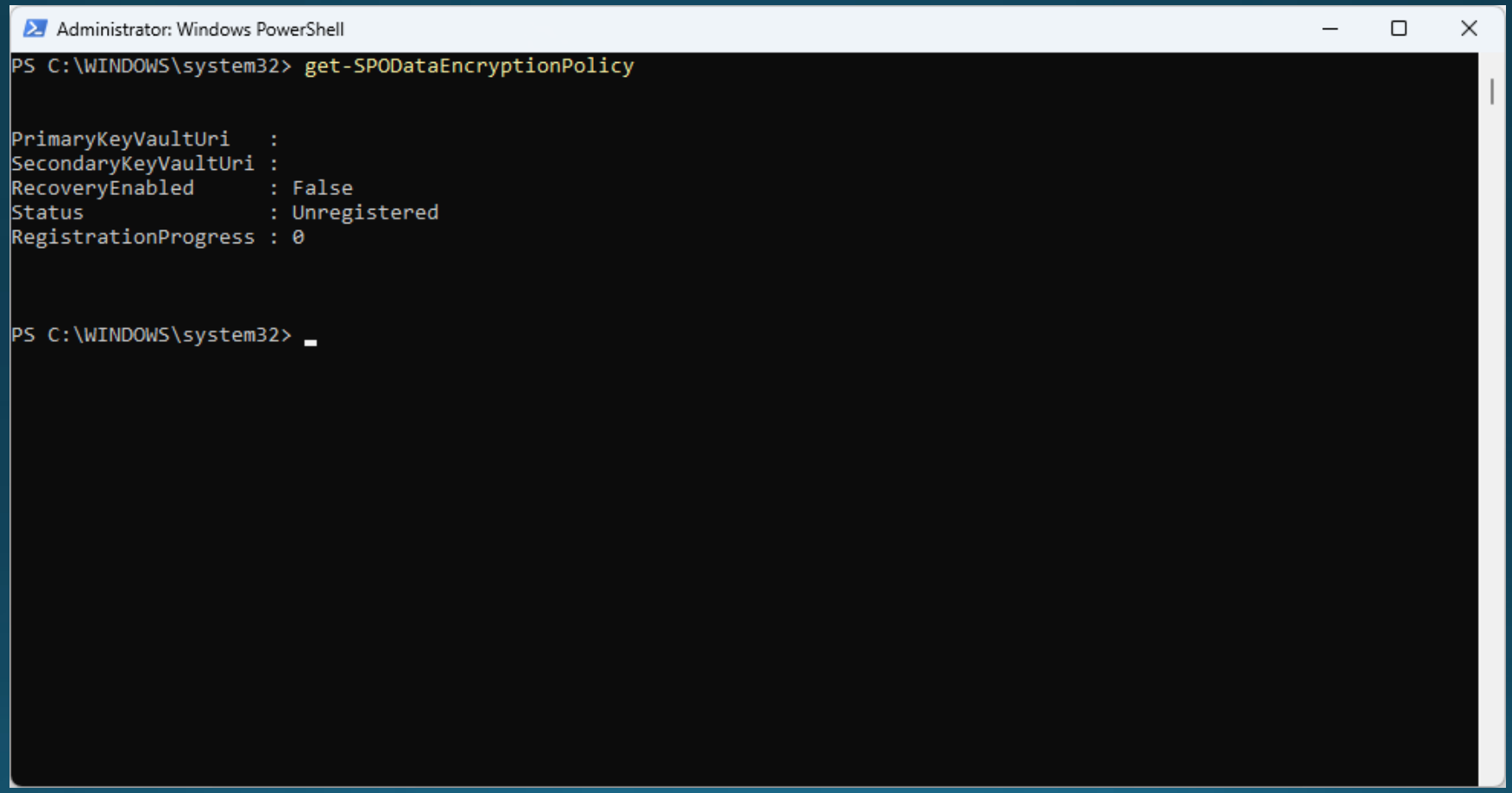
The Microsoft 365 Customer Key Onboarding Service is a service that allows you to enable Customer Key within your own tenant. This feature automatically validates the required Customer Key resources. If desired, you can validate your resources separately before proceeding with Customer Key enablement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

Important

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

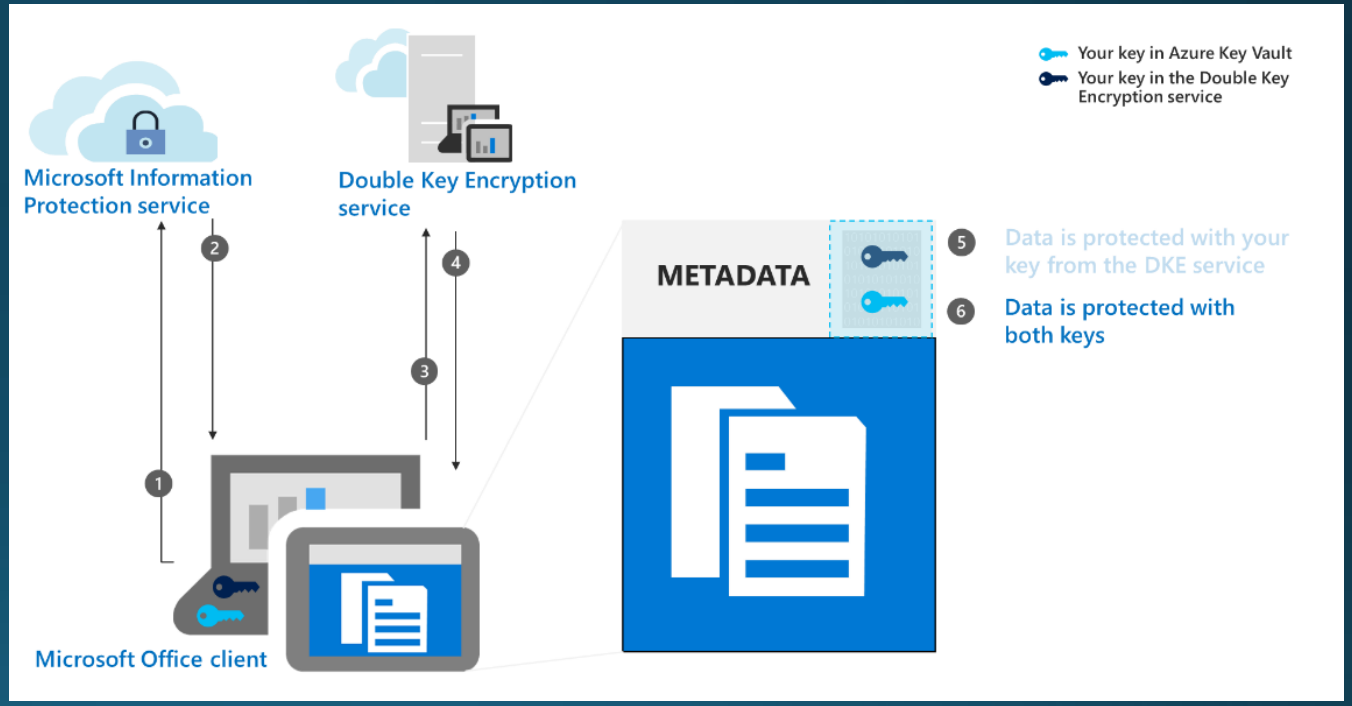
- Government tenants - see "Onboard to Customer Key for Government tenants" below.
- SharePoint and OneDrive - see "Onboard to Customer Key for SharePoint and OneDrive" below.
- Tenants using managed HSMs - see "Onboard to Customer Key using the legacy method" below.

Customer Key status



Double Key Encryption

- Office Apps | Sensitivity labels
- Tenant key and organizational key
- Impairs specific functions

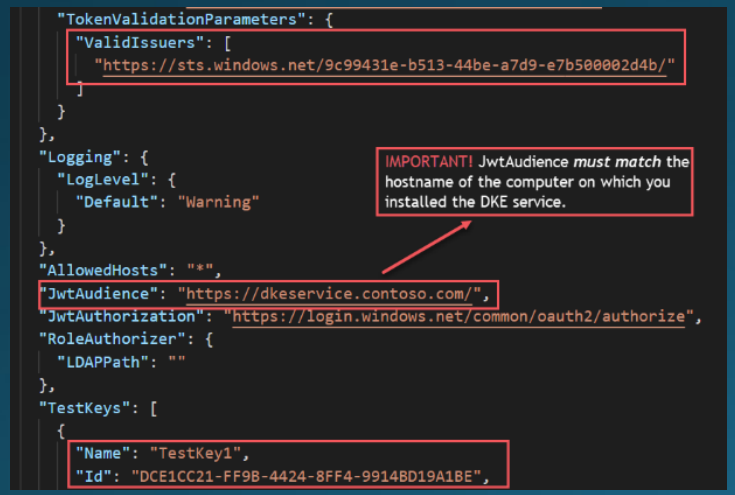


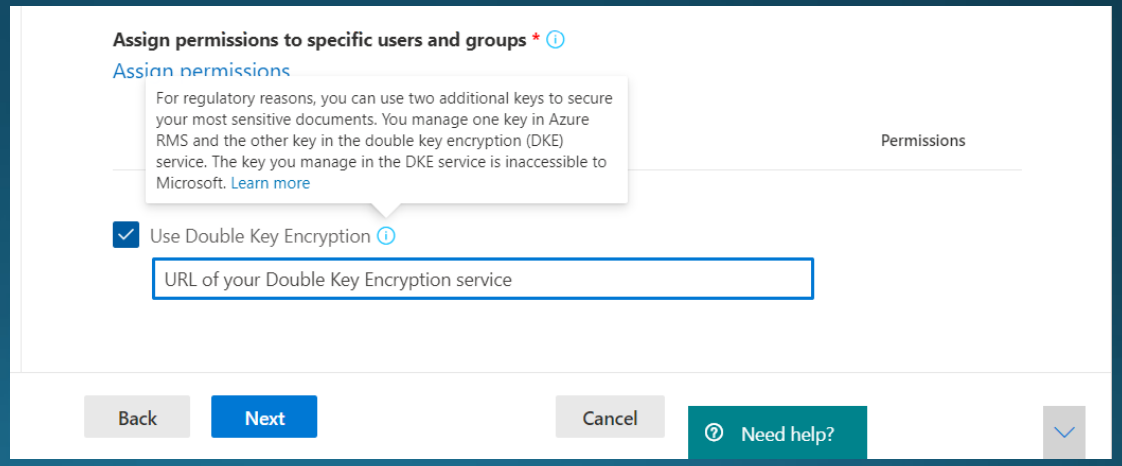
Double Key Encryption

Software DKE service, GitHub

Deploy service, publish key

Create labels with DKE





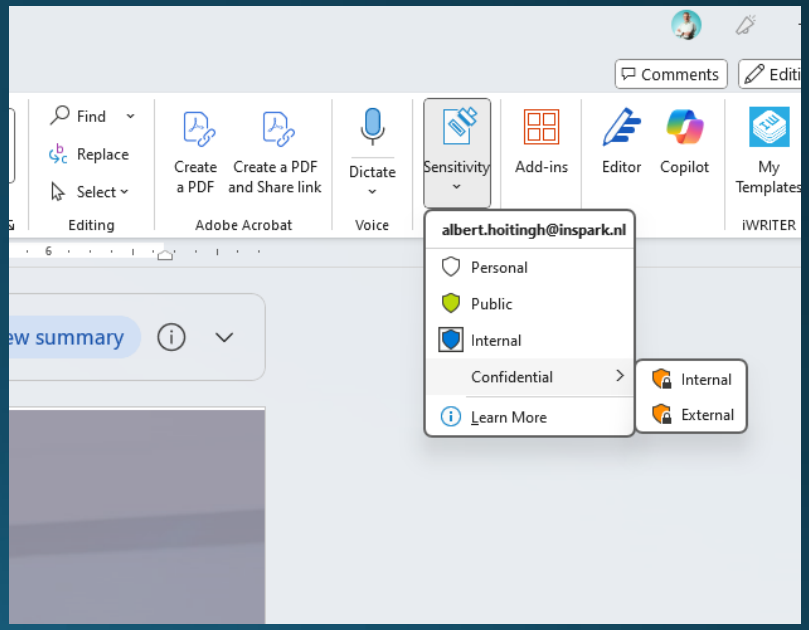
Sensitivity labels

Items and labels

Label stays with item

Encryption |
Visual markings |
Offline availability

Hierarchy is important



https://learn.microsoft.com/en-us/purview/technical-reference-details-about-encryption

Encryption standards

1

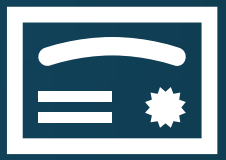
Content key

Symmetric AES256-CBC
(Cypher Block Chaining)

2

Key protection

Asymmetric
RSA 2048 bit

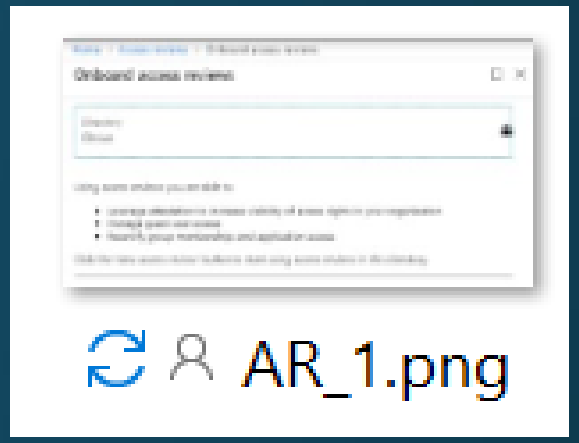


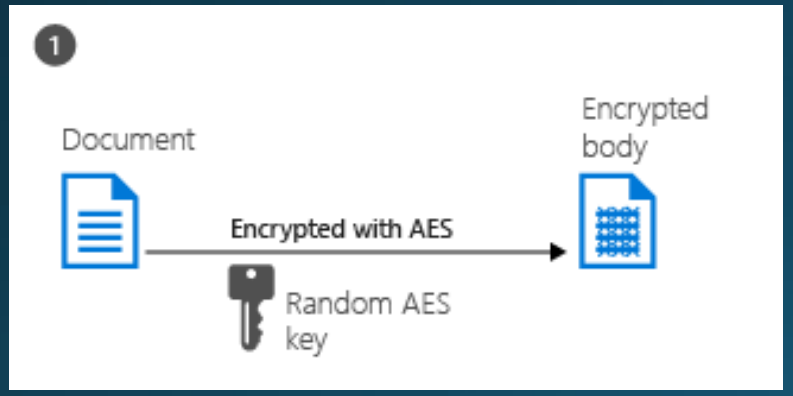
3

Certificate signing

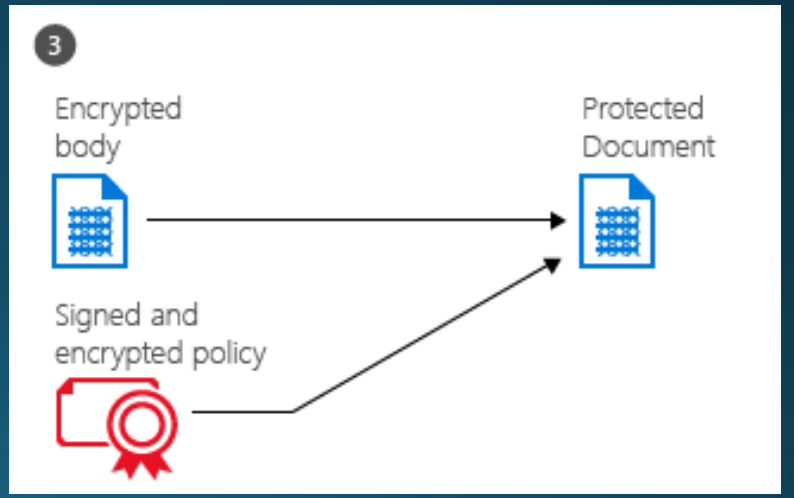
SHA-256

How it works

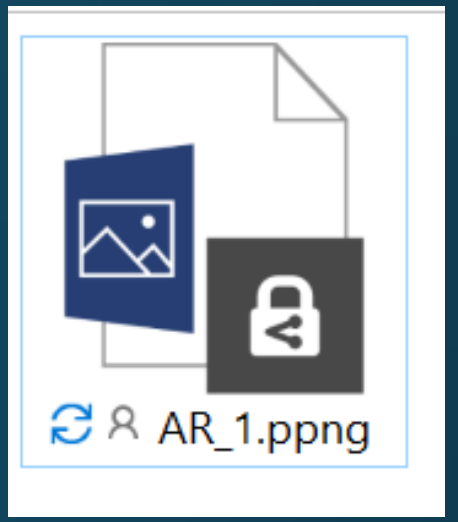

AR_1.png

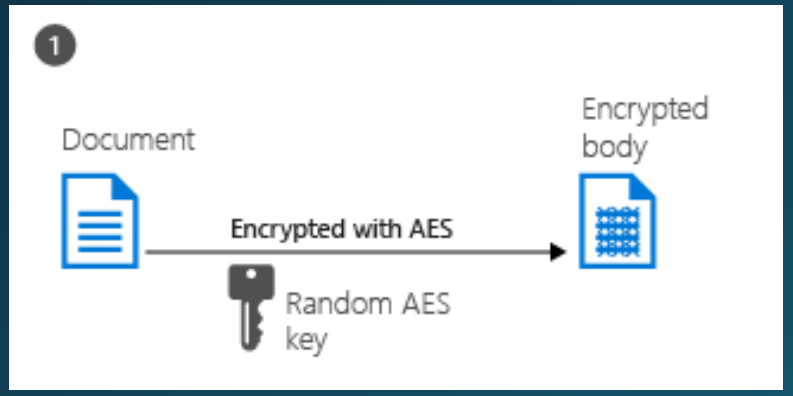

1
Document
Encrypted body
Encrypted with AES
Random AES key


2
AES key
New Policy
Encrypt with organization's public key
Signed and encrypted policy
Sign with user's private key
Rights:
Marketing: read
Engineering: edit
Expiration: 1/1/2030

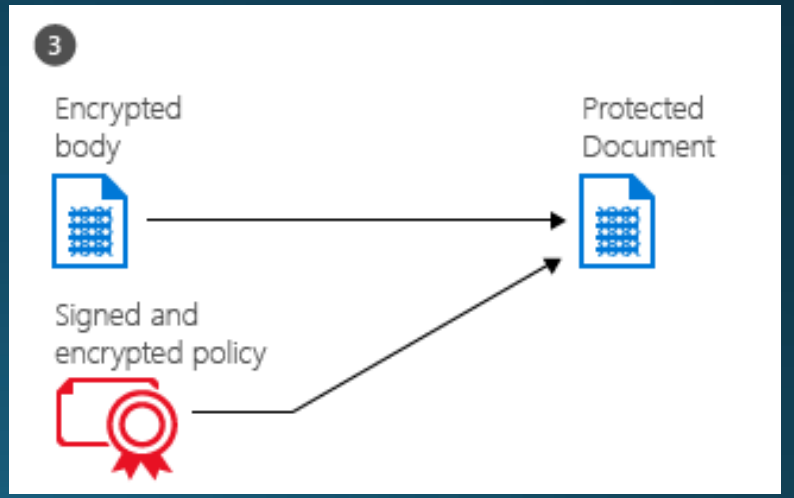

3
Encrypted body
Protected Document
Signed and encrypted policy

How it works


AR_1.ppng


1
Document
Encrypted body
Encrypted with AES
Random AES key


2
AES key
New Policy
Encrypt with organization's public key
Signed and encrypted policy
Sign with user's private key
Rights:
Marketing: read
Engineering: edit
Expiration: 1/1/2030

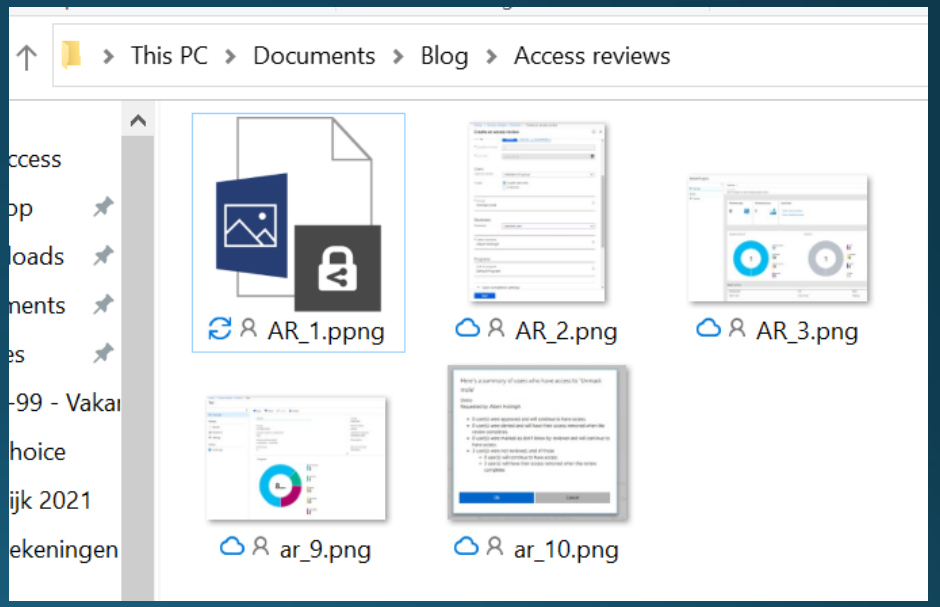

3
Encrypted body
Protected Document
Signed and encrypted policy

Filetypes are important

Native clients | Microsoft Edge

Microsoft Purview Information Protection Viewer client

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

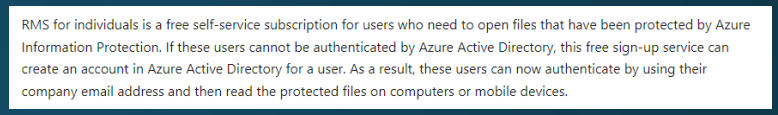


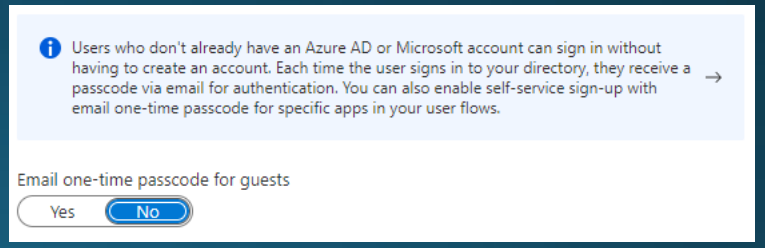
Identities are important

Entra ID accounts

Microsoft Live | Guest | RMS

Set-SPOTenant -EnableAzureADB2BIntegration

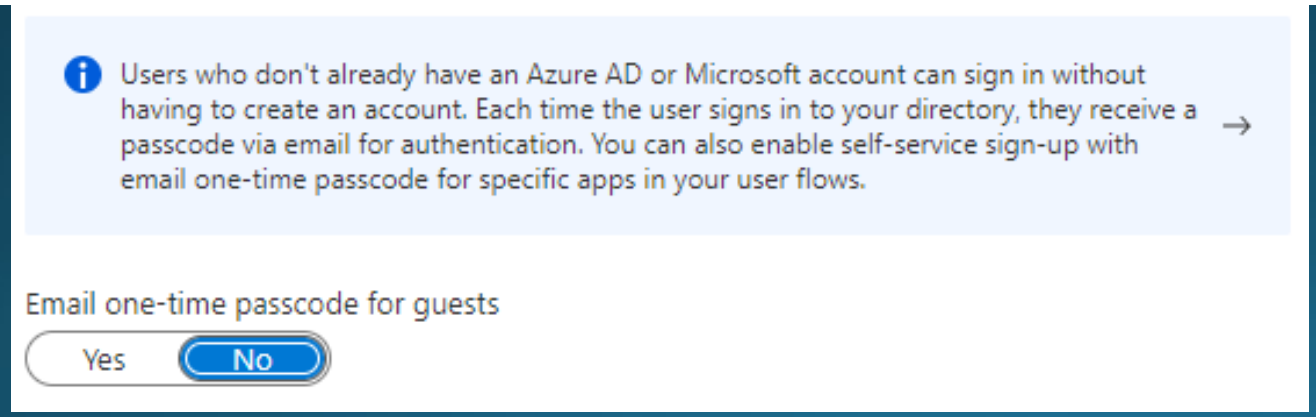




Identities are important

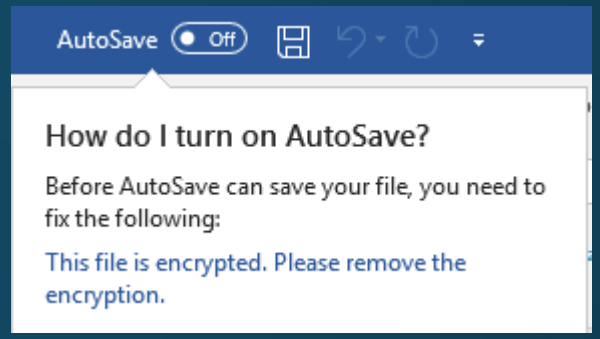
Entra ID accounts

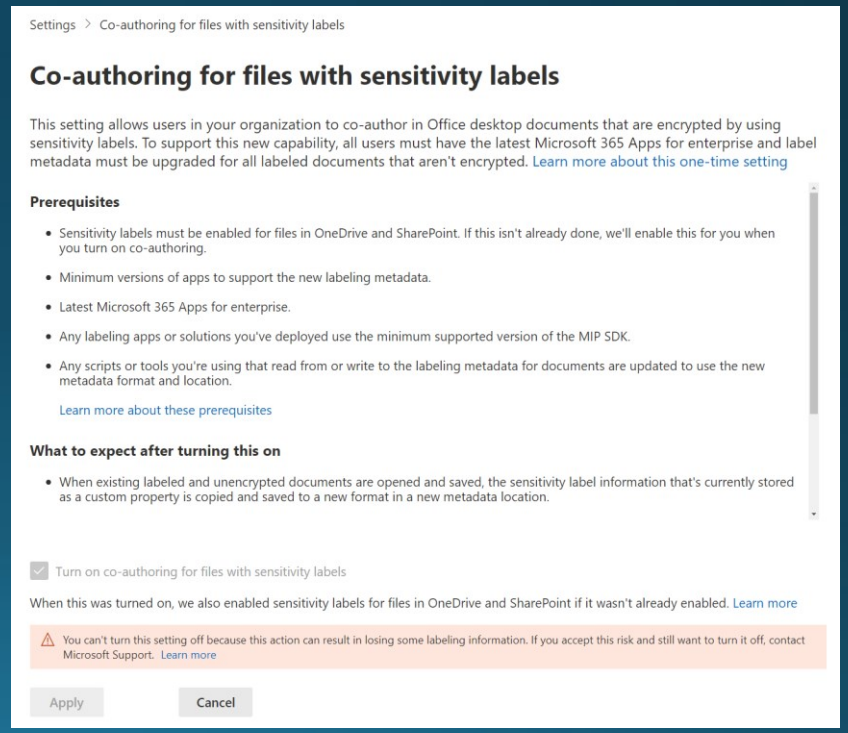
RMS for individuals is a free self-service subscription for users who need to open files that have been protected by Azure Information Protection. If these users cannot be authenticated by Azure Active Directory, this free sign-up service can create an account in Azure Active Directory for a user. As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



Consequences

- Co-authoring | auto-save
- eDiscovery | content search
- Microsoft 365 Copilot





Consequences

Co-authoring | auto-save

eDiscovery | content search

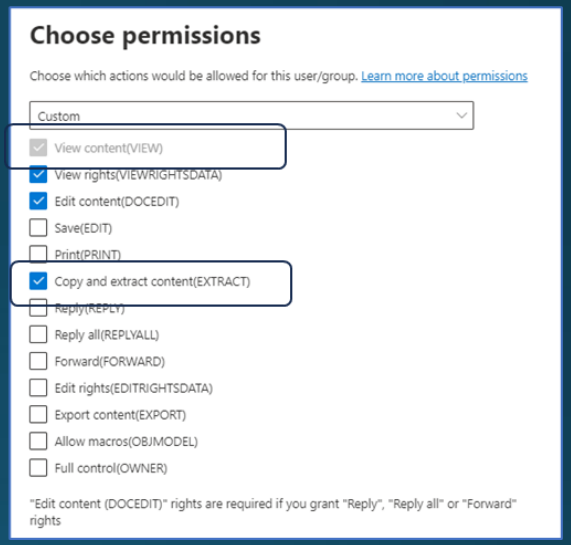
Microsoft 365 Copilot

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 ⓘ

Never

Allow offline access ⓘ

Always

Assign permissions to specific users and groups * ⓘ

Assign permissions

1 item

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

☐ Use Double Key Encryption ⓘ

Assign permissions now or let users decide?

Let users assign permissions when they apply the label

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

Encrypt-Only

In Word, PowerPoint, and Excel, prompt users to specify permissions

Use Double Key Encryption

Permissions

Specify who can do what

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.

A albert.hoitingh@inspark.nl

More Options

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)
- [x] 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

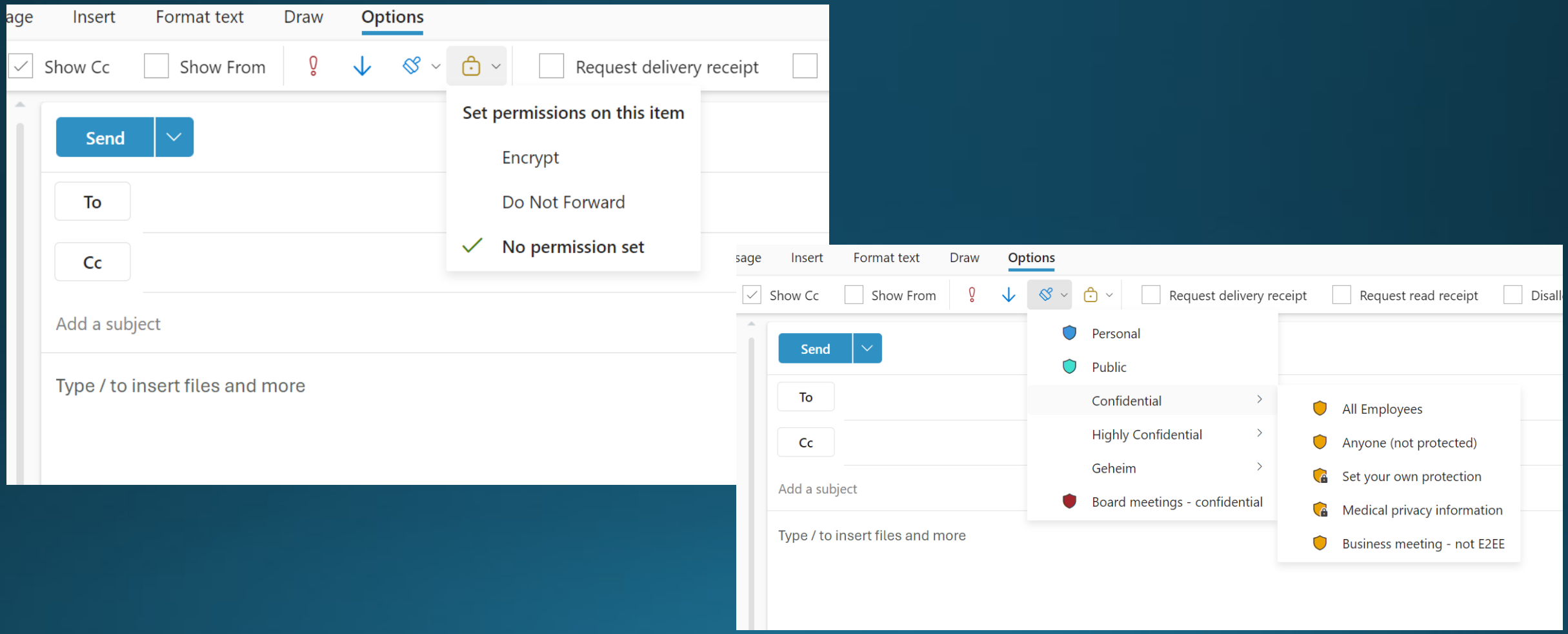
Co-Owner

- 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



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

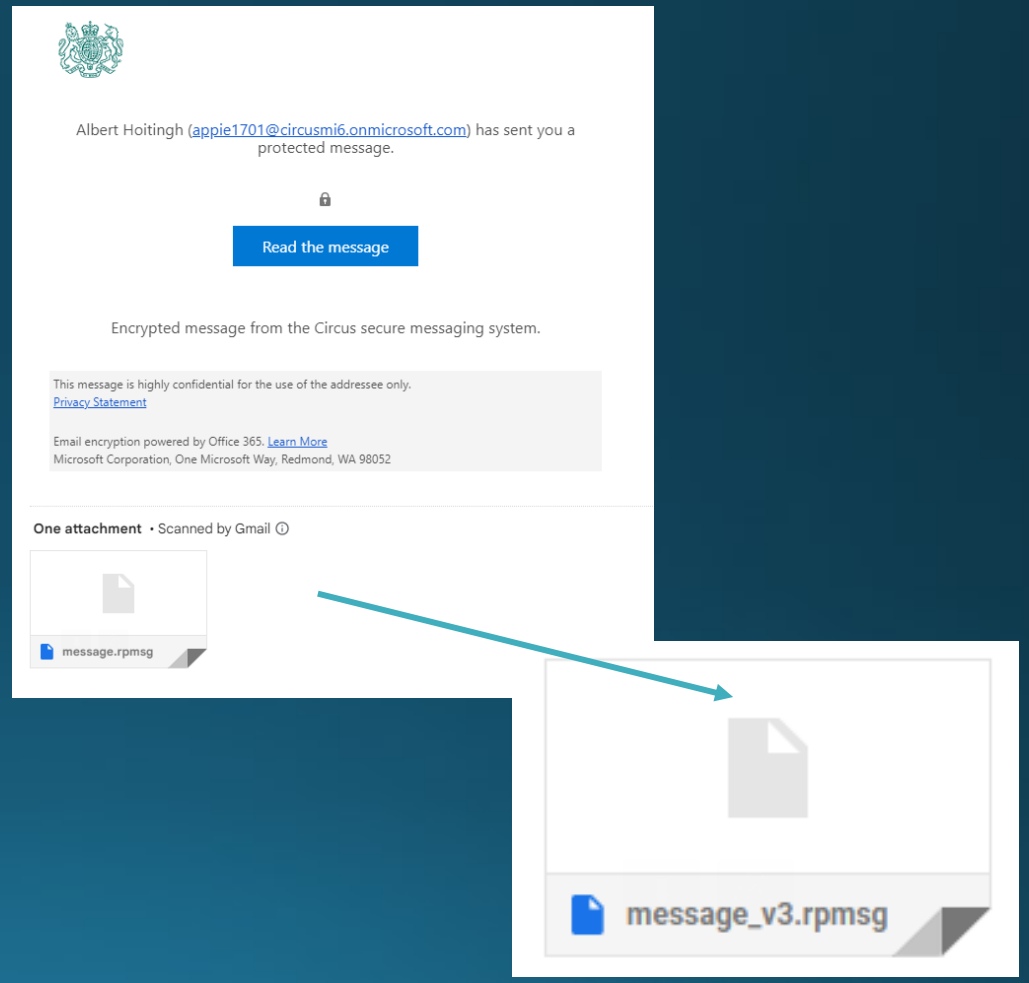
E5 - Information Protection and Governance

E5 - Compliance

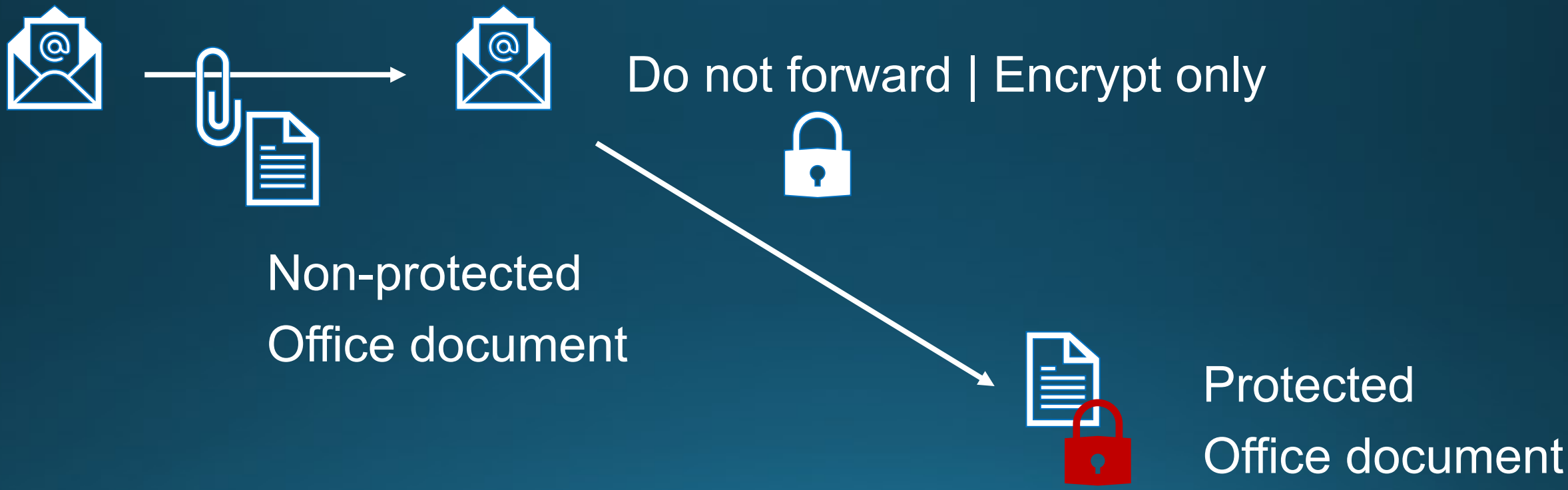
E5

Encapsulated e-mail message

- .pmsg file
- Outlook: opens natively
- Secure web-portal
- MPIP viewer does not work

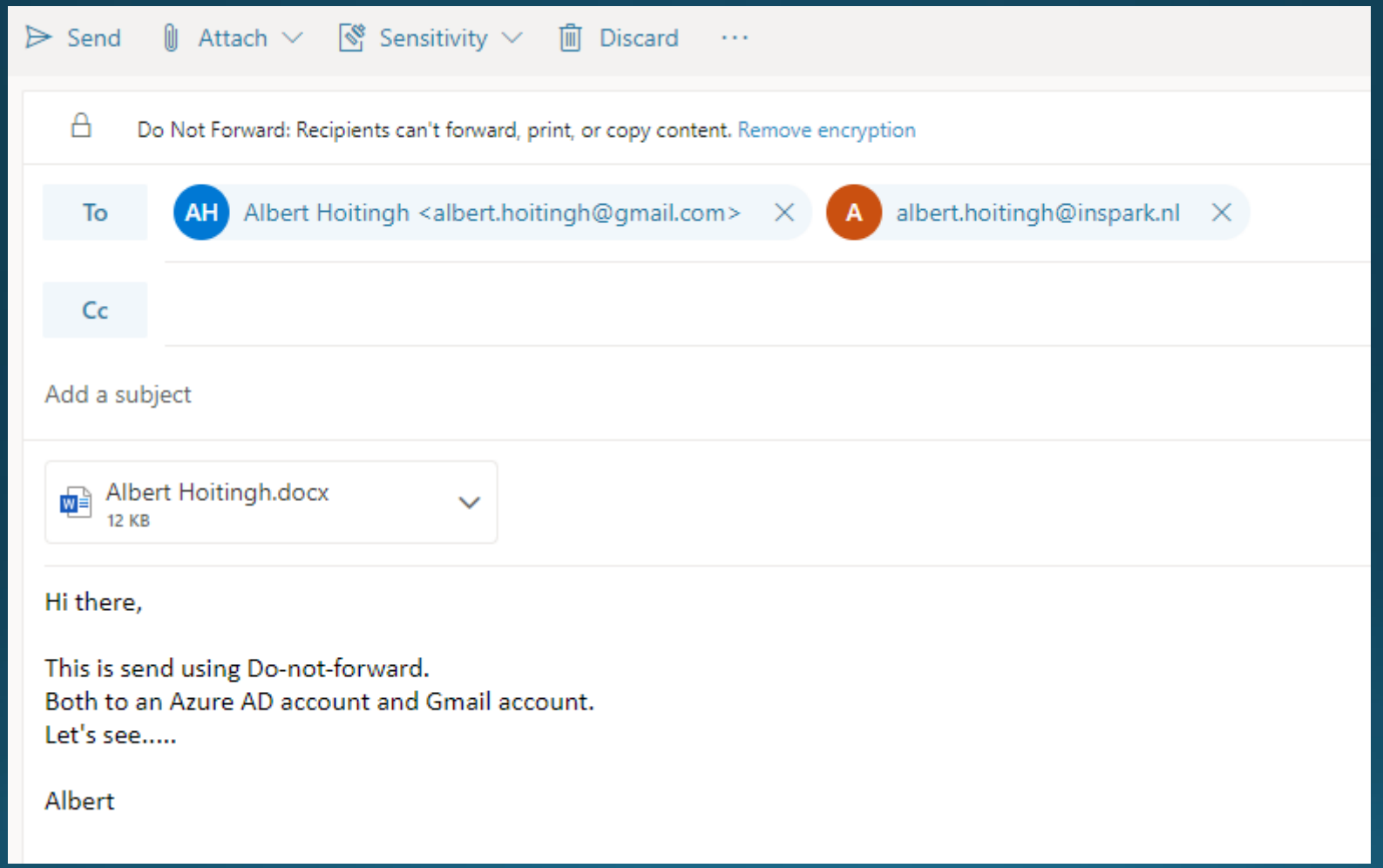


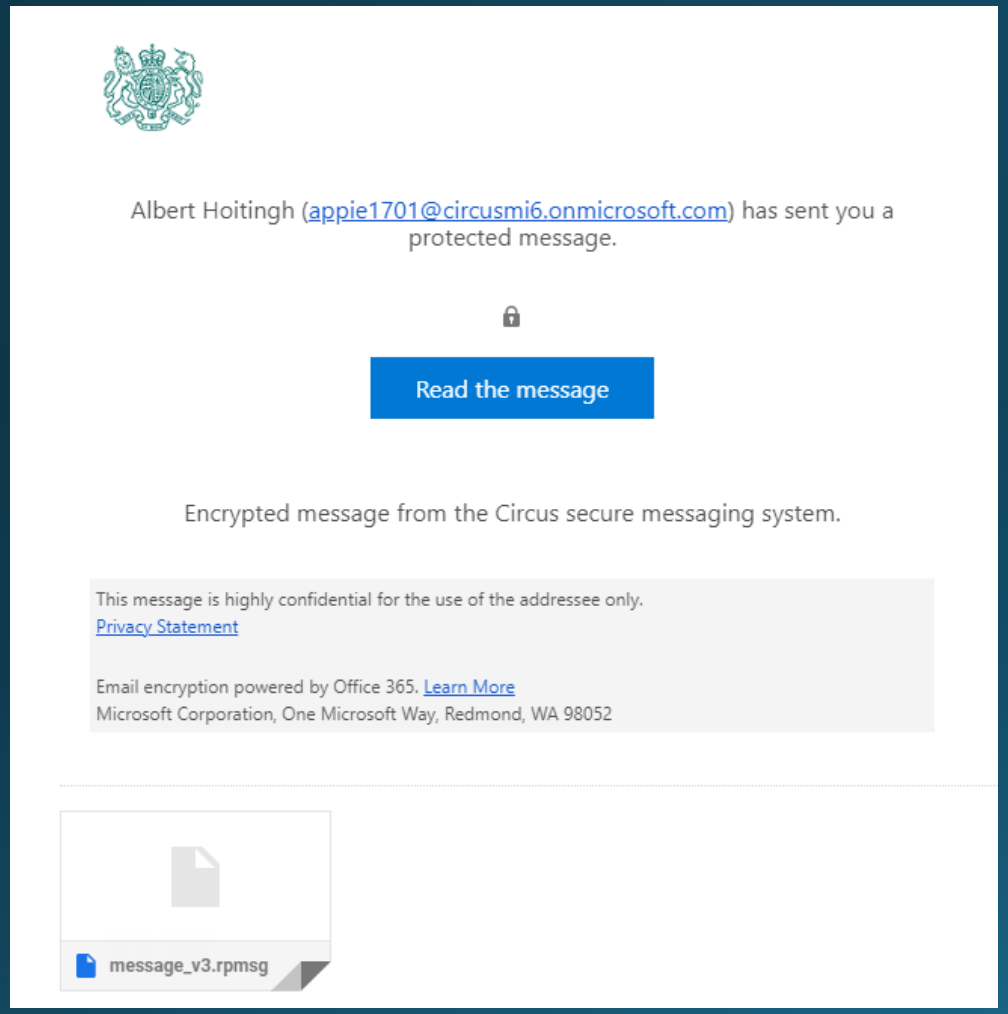
E-mail attachments

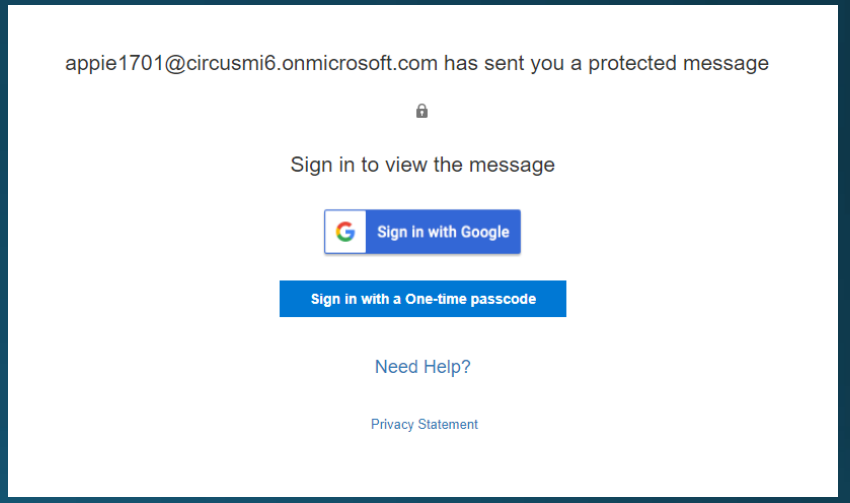


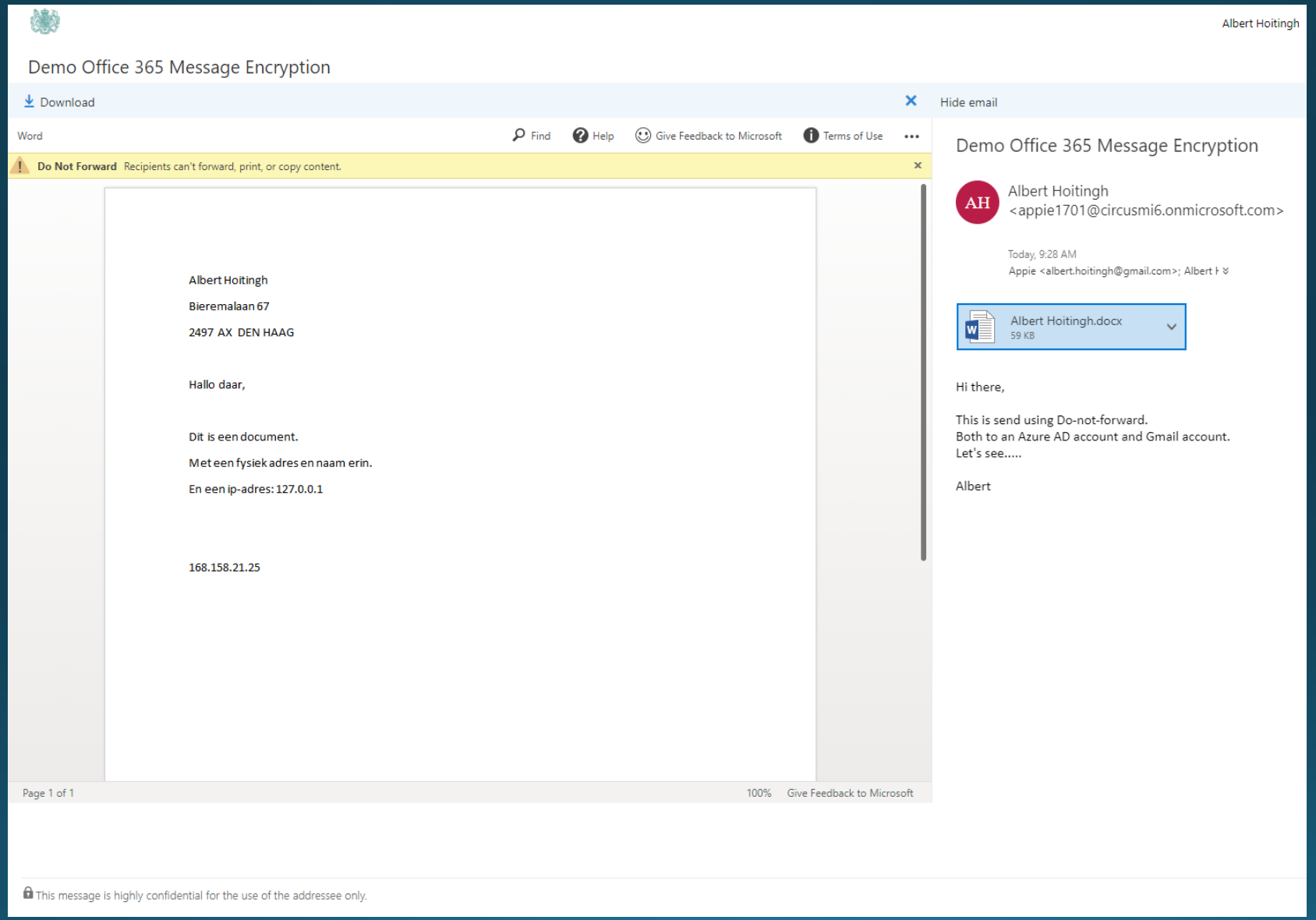
Mind the Entra ID account
Set-IRMConfiguration - DecryptAttachmentForEncryptOnly <$true|$false>

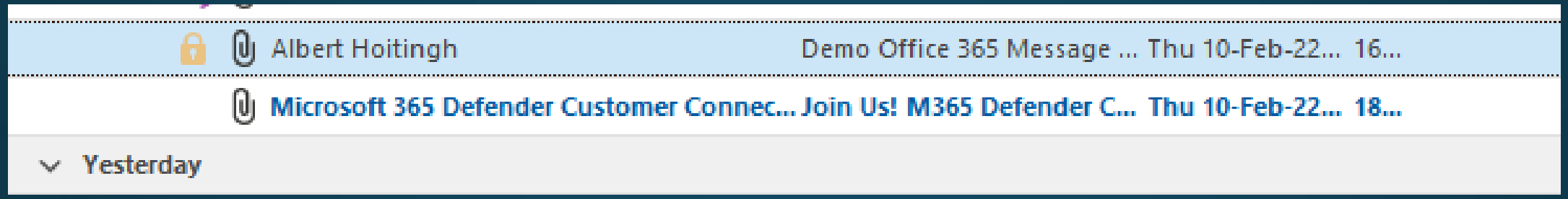
Run-through Message Encryption


Send
Attach
Sensitivity
Discard
Do Not Forward: Recipients can't forward, print, or copy content. Remove encryption
To
AH
Albert Hoitingh <albert.hoitingh@gmail.com>
A
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
message_v3.rpmsg


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


Albert Hoitingh
Demo Office 365 Message Encryption
Download
Hide email
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
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
This message is highly confidential for the use of the addressee only.



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

AH

Albert Hoitingh <appie1701@circusmi6.onmicrosoft.com>

To Appie; Albert Hoitingh

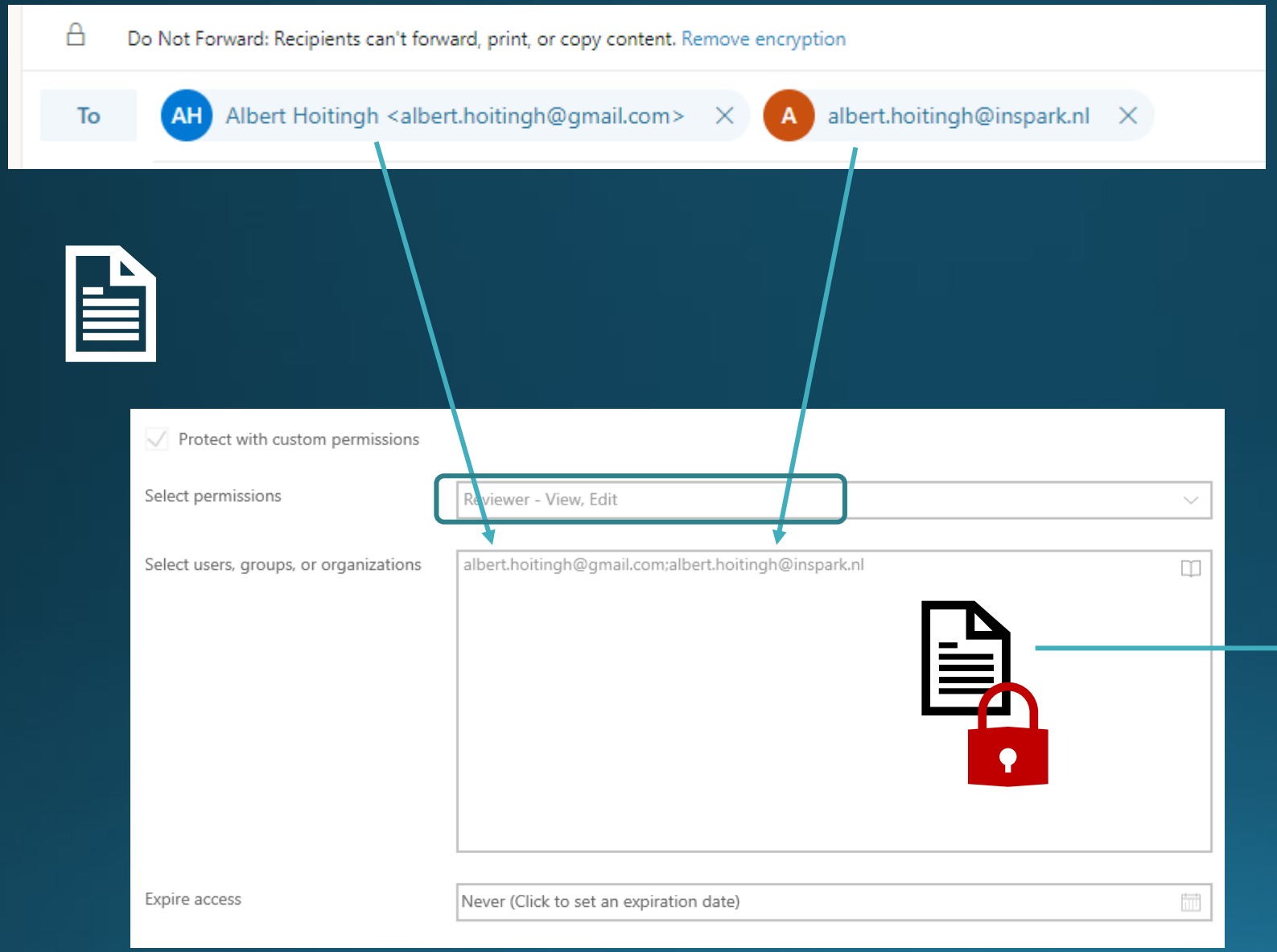
Do Not Forward - Recipients can't forward, print, or copy content.
Permission granted by: appie1701@circusmi6.onmicrosoft.com
If there are problems with how this message is displayed, click here to view it in a web browser.

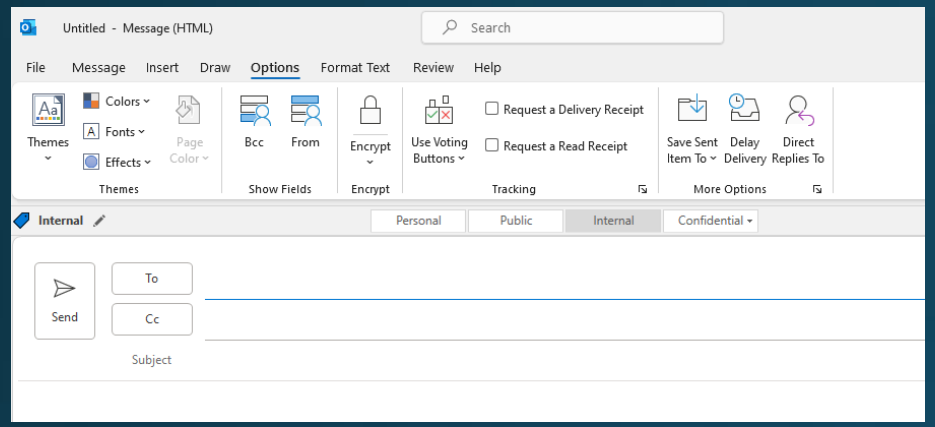
Albert Hoitingh.docx
59 KB

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
AH
Albert Hoitingh <albert.hoitingh@gmail.com>
A
albert.hoitingh@inspark.nl
Protect with custom permissions
Select permissions
Reviewer - View, Edit
Select users, groups, or organizations
albert.hoitingh@gmail.com;albert.hoitingh@inspark.nl
Expire access
Never (Click to set an expiration date)
My Permission
You are currently authenticated to view this document as:
albert.hoitingh@inspark.nl
Do Not Forward - Recipients can't forward, print, or copy content.
You have the following permissions:
View: Yes
Edit: Yes
Copy: No
Print: No
Save: Yes
Export: No
Access the document programmatically: Yes
Full control: No
Request additional permissions...
OK



You don't have permission to view this message

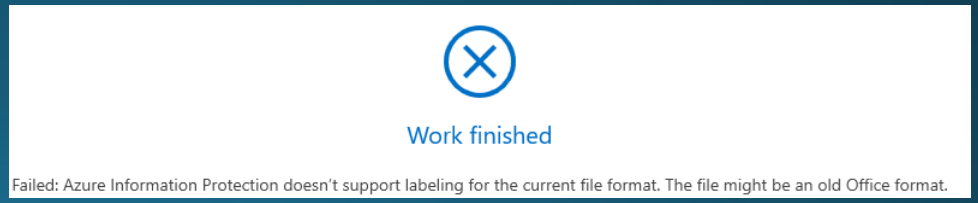
This message is protected and you don't have permission to view it.

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

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



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