

TeleTrust-EBCA "PKI-Workshop" 2020

Berlin, 01.10.2020

"Einblicke in OME, AIP und RMS - macht Microsoft 365 die E-Mail-Verschlüsselung obsolet?"

Thomas Welslau, Net at Work

Begrifflichkeiten

CYOK

AIP

RMS

BYOK

Cybersecurity Reference Architecture

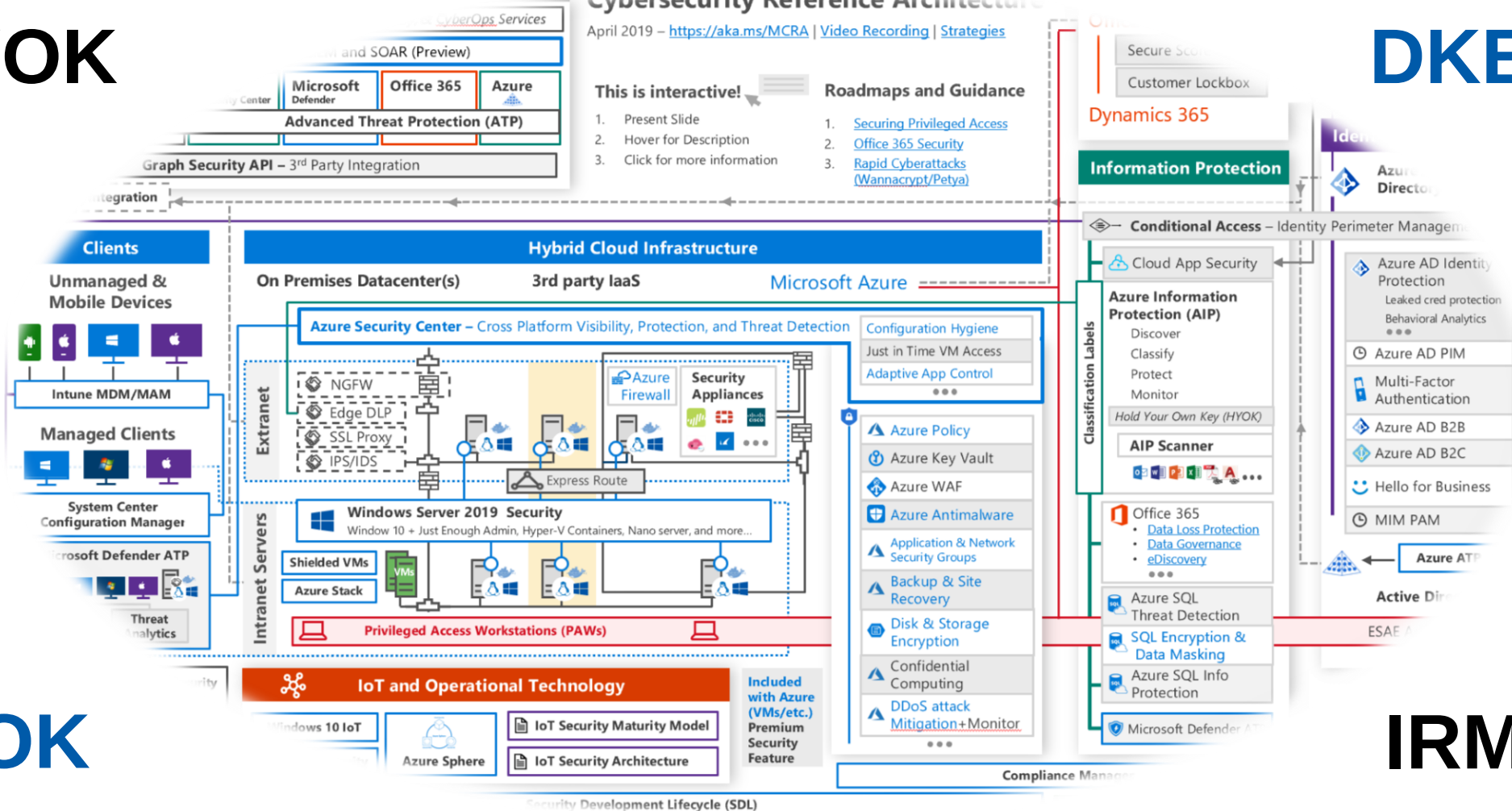
April 2019 – <https://aka.ms/MCRA> | [Video Recording](#) | [Strategies](#)

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Roadmaps and Guidance

1. [Securing Privileged Access](#)
2. [Office 365 Security](#)
3. [Rapid Cyberattacks \(Wannacrypt/Petya\)](#)



DKE

OME

HYOK

IRM



Azure Information Protection

- Klassifizieren und Schützen von Dokumenten
- Automatische Anwendung von Labels oder durch Benutzerzuweisung
- Der Zugriff auf Dokumente kann im Nachgang zurück gezogen werden

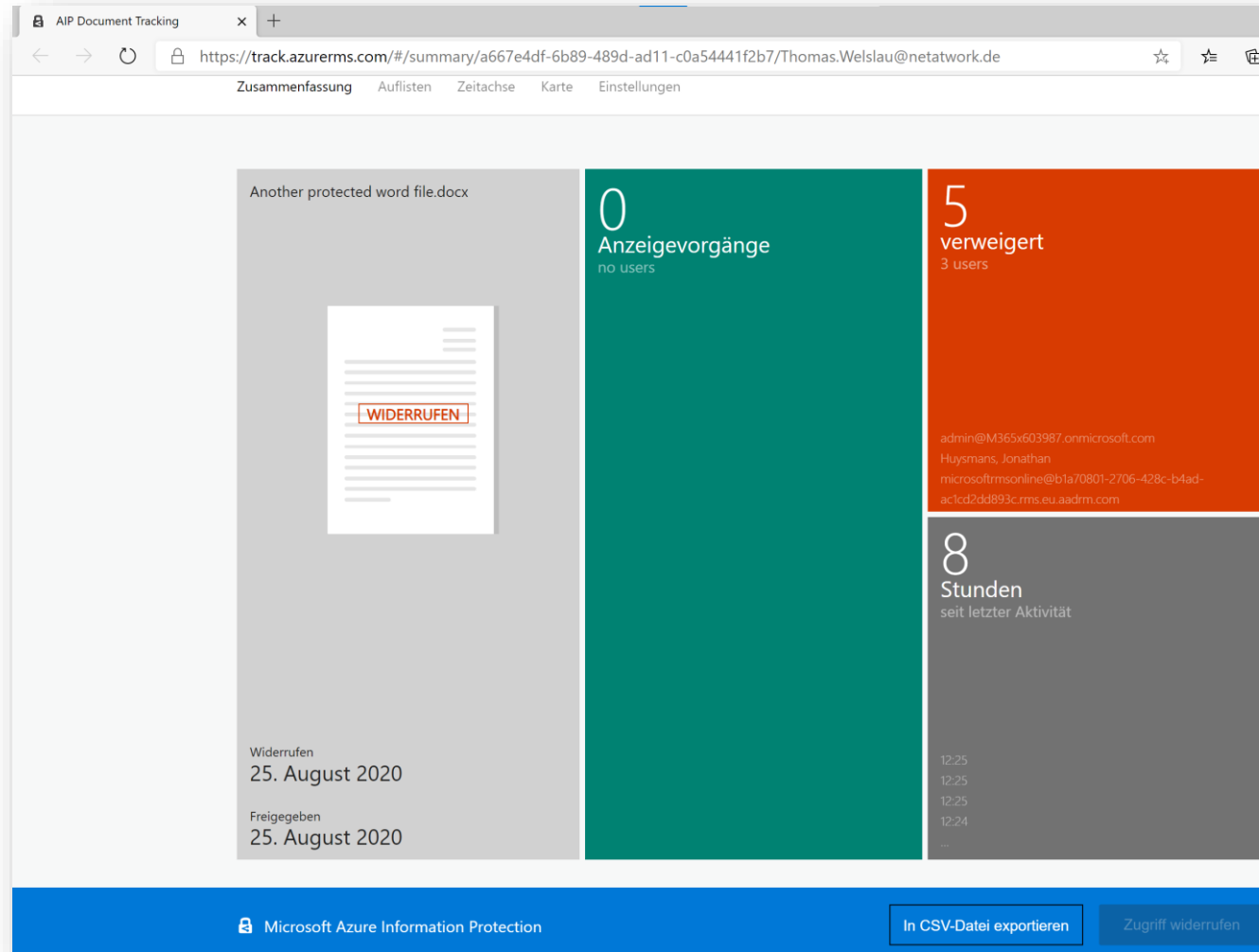
- Verschlüsselung von E-Mails
- Automatisch über Transportregeln oder durch Auswahl im E-Mail Client



Office 365 Nachrichtenverschlüsselung

- Beide Funktionen nutzen als Grundlage den Azure Rights Management Service (Azure RMS)
- Der Dokumentenschutz kann mit Nutzungsrechten kombiniert werden

Zugriff widerrufen



AIP Document Tracking

https://track.azureinfo.com/#/summary/a667e4df-6b89-489d-ad11-c0a54441f2b7/Thomas.Welslau@netatwork.de

Zusammenfassung Auflisten Zeitachse Karte Einstellungen

Another protected word file.docx

WIDERRUFEN

Widerrufen
25. August 2020

Freigegeben
25. August 2020

0
Anzeigevorgänge
no users

5
verweigert
3 users

admin@M365x603987.onmicrosoft.com
Huysmans, Jonathan
microsoftsonline@b1a70801-2706-428c-b4ad-
ac1cd2dd893c.ms.eu.aadm.com

8
Stunden
seit letzter Aktivität

12:25
12:25
12:25
12:24

Microsoft Azure Information Protection

In CSV-Datei exportieren

Zugriff widerrufen

Labels zur Verschlüsselung

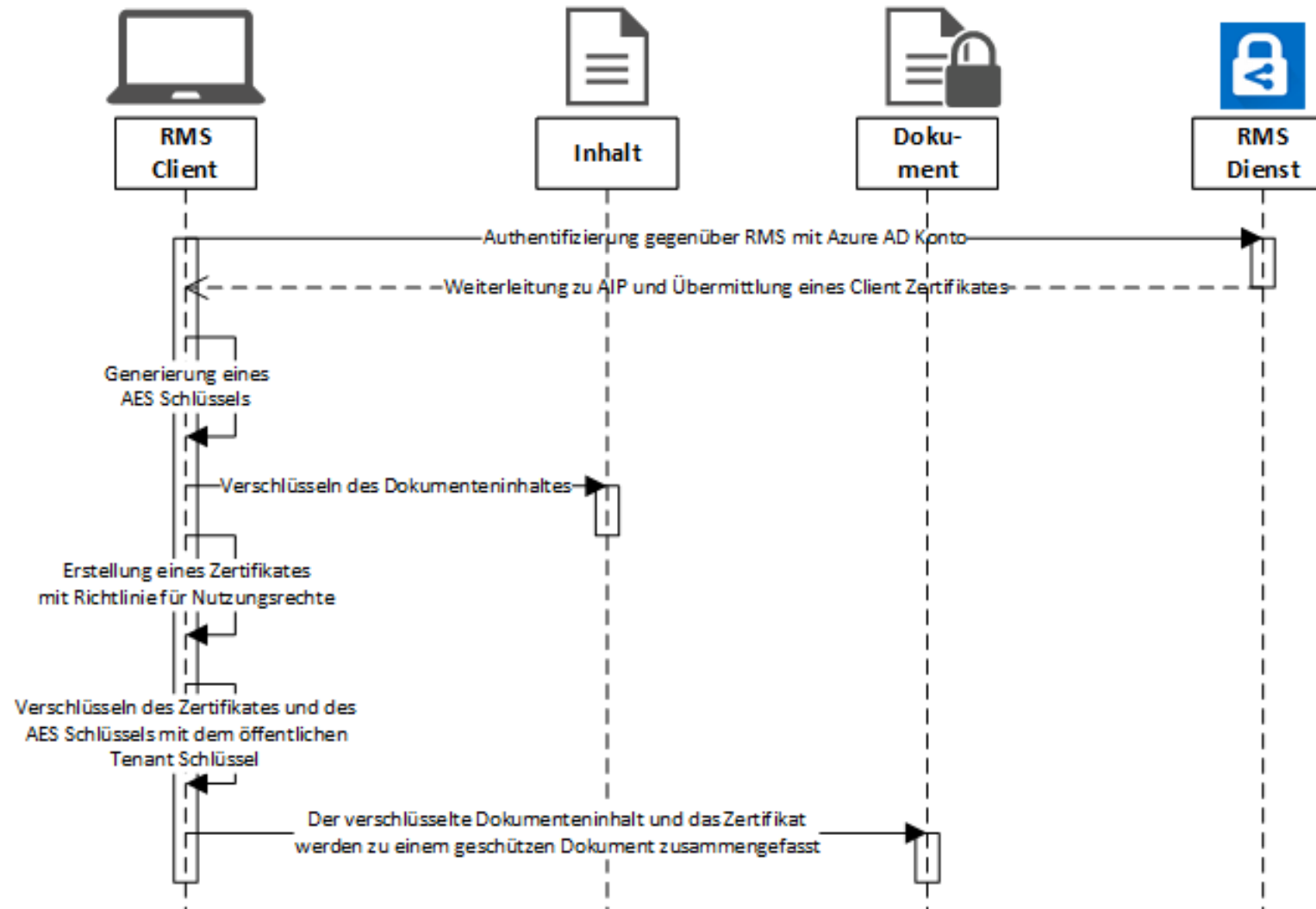
Azure Information Protection Labels

Label display name	Policy	Marking	Protection
■ Vertraulich innerhalb der Organisation	Global	✓	...
■ Vertraulich nur Empfänger	Global	✓	...
∨ Protection templates			...
Confidential \ All Employees		✓	...
Highly Confidential \ All Employees		✓	...

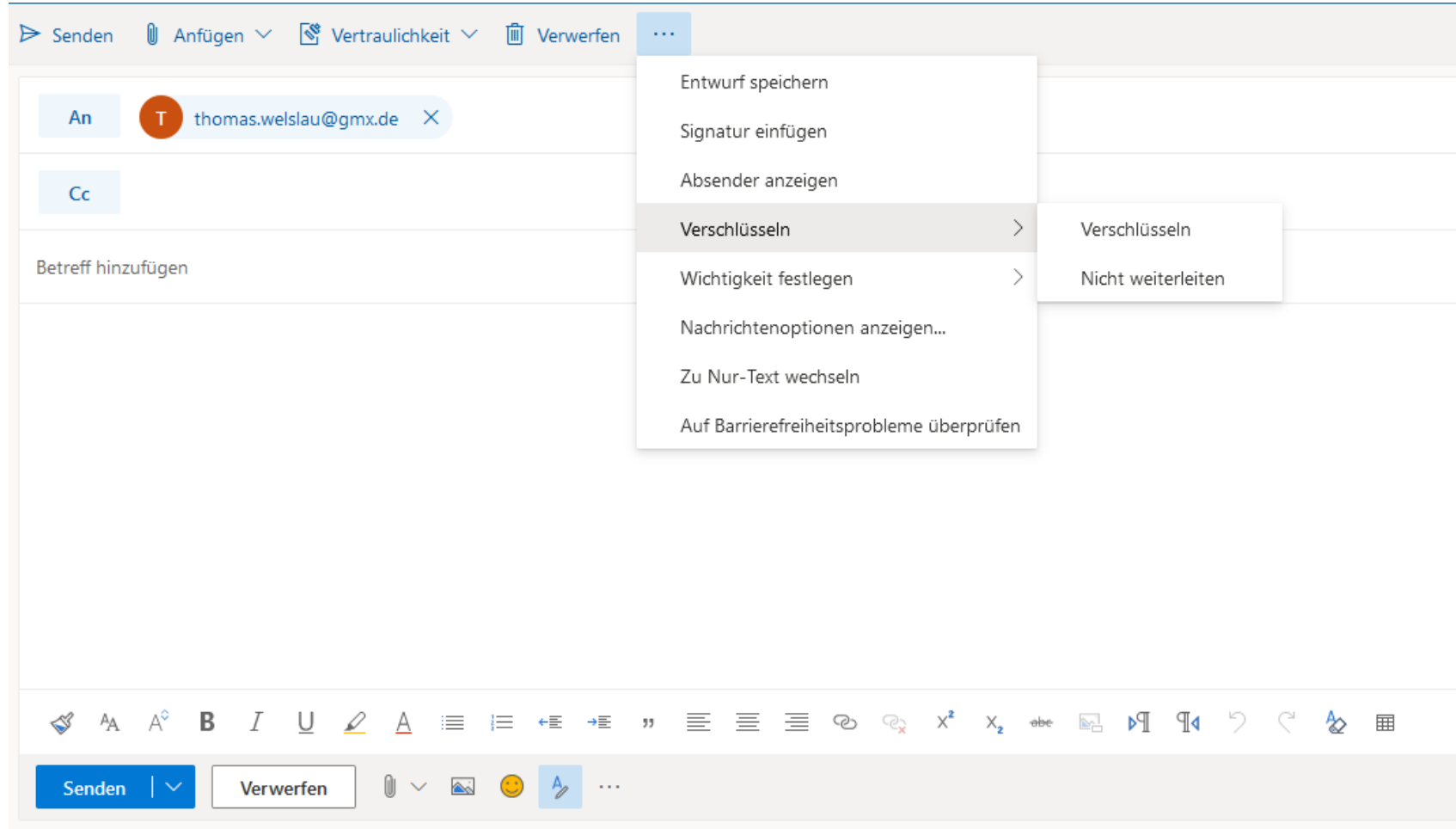
Office 365 Nachrichtenverschlüsselung Templates

```
PS C:\Users\twelslau> Get-RMSTemplate_
Name
----
Confidential \ All Employees Confidential data that requires protection, which allows all employees full permissions. Data owners can track and revoke content.
Highly Confidential \ All Employees Highly confidential data that allows all employees view, edit, and reply permissions to this content. Data owners can track and revoke content.
Verschlüsseln Diese Nachricht ist verschlüsselt. Empfänger können die Verschlüsselung nicht entfernen.
Nicht weiterleiten Empfänger können nicht weiterleiten, drucken oder Inhalt kopieren.
```

RMS als Grundlage - Verschlüsselung



E-Mail verschlüsseln - Client



E-Mail verschlüsseln - Transportregel

Neue Regel

Name:

Gesendet an 'thomas.welslau@netatwork.de'

*Diese Regel anwenden, wenn...

Der Empfänger ist...

['thomas.welslau@netatwork.de'](#)

Bedingung hinzufügen

*Folgendermaßen vorgehen...

Office 365-Nachrichtenverschlüsselung und -Rechtsschutz anwenden auf die Nachricht mit...

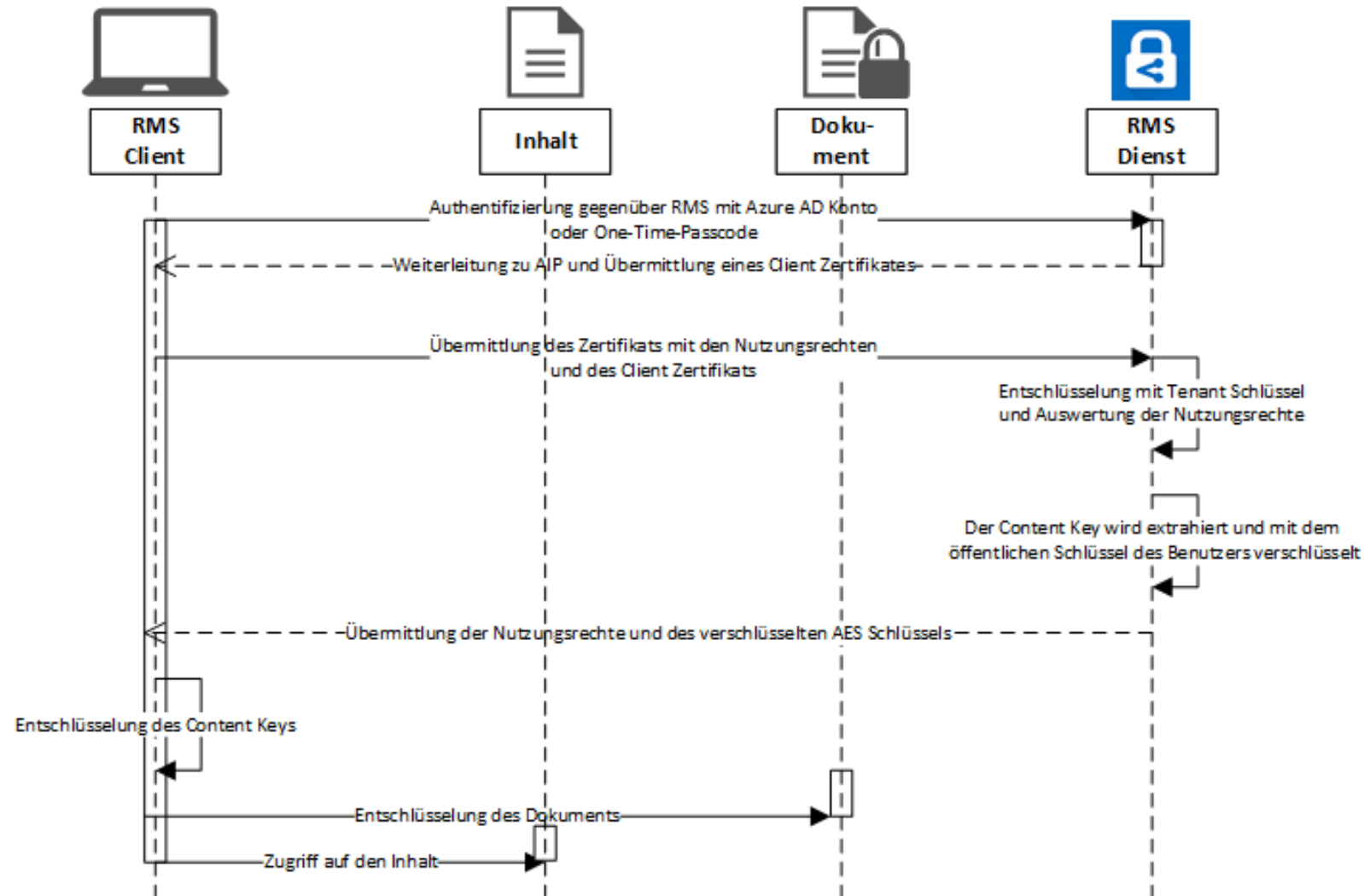
[Verschlüsseln NAW](#)

Aktion hinzufügen

Außer wenn...

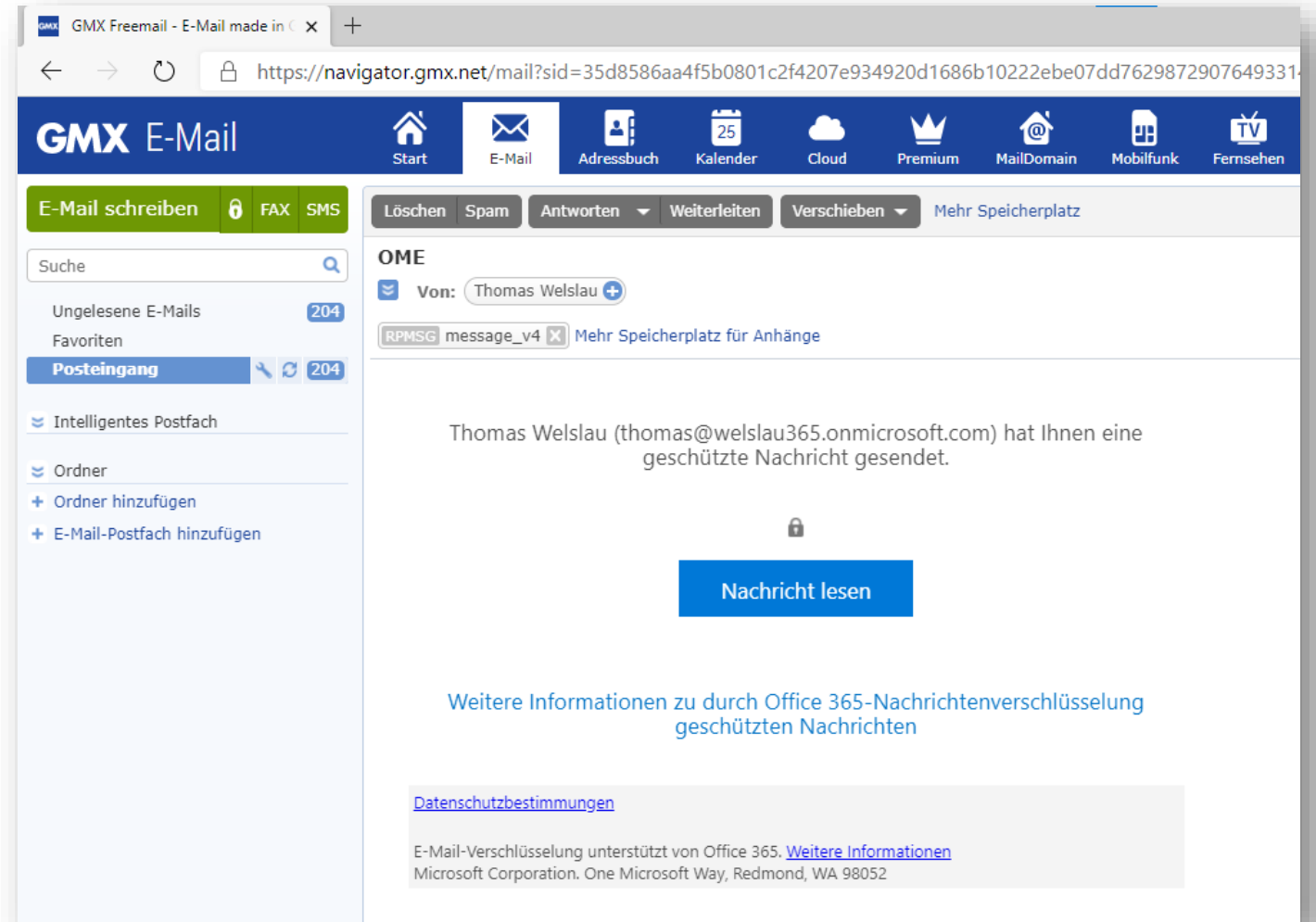
Ausnahme hinzufügen

RMS als Grundlage - Entschlüsselung

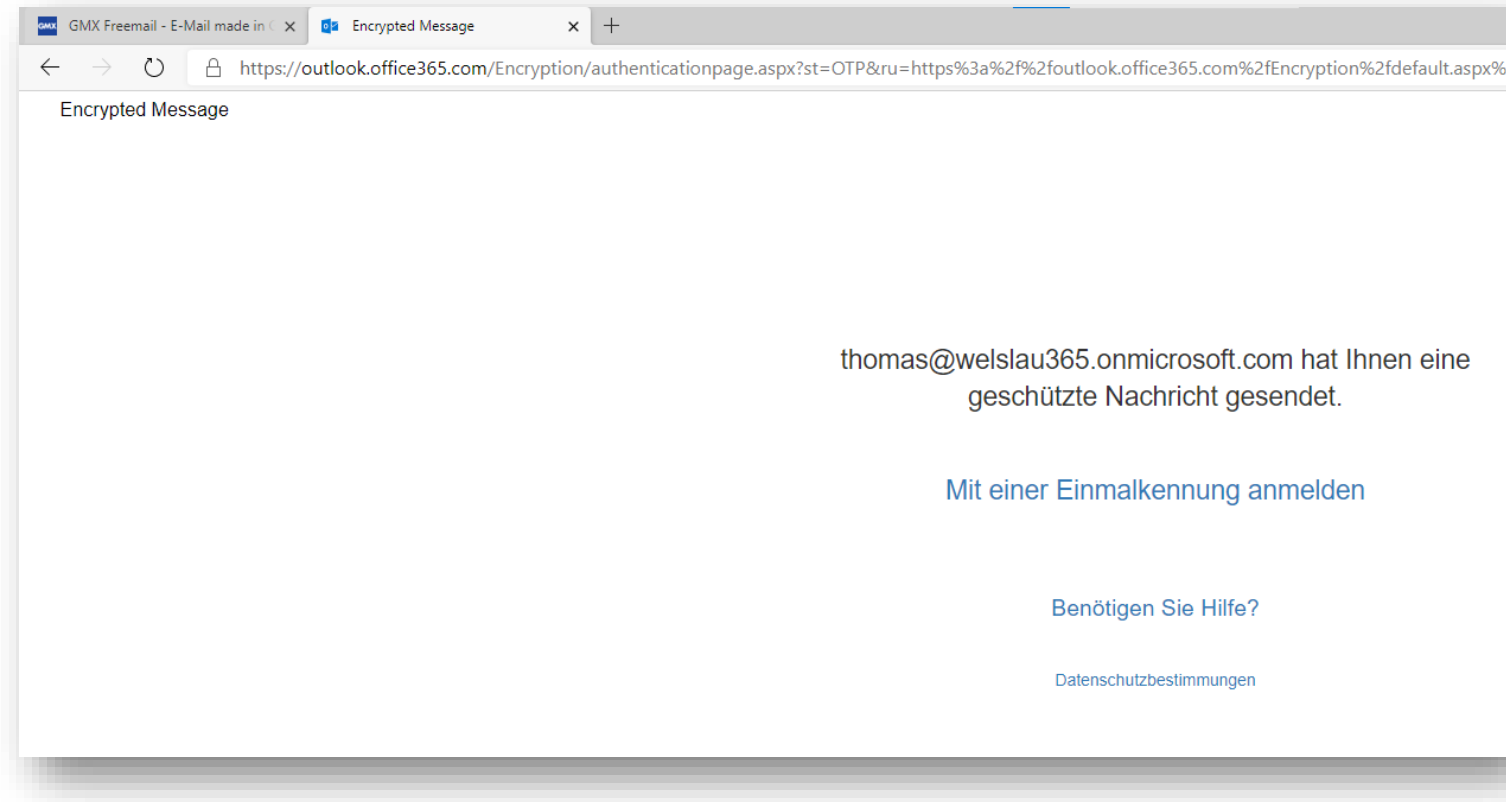


Nachricht entschlüsseln

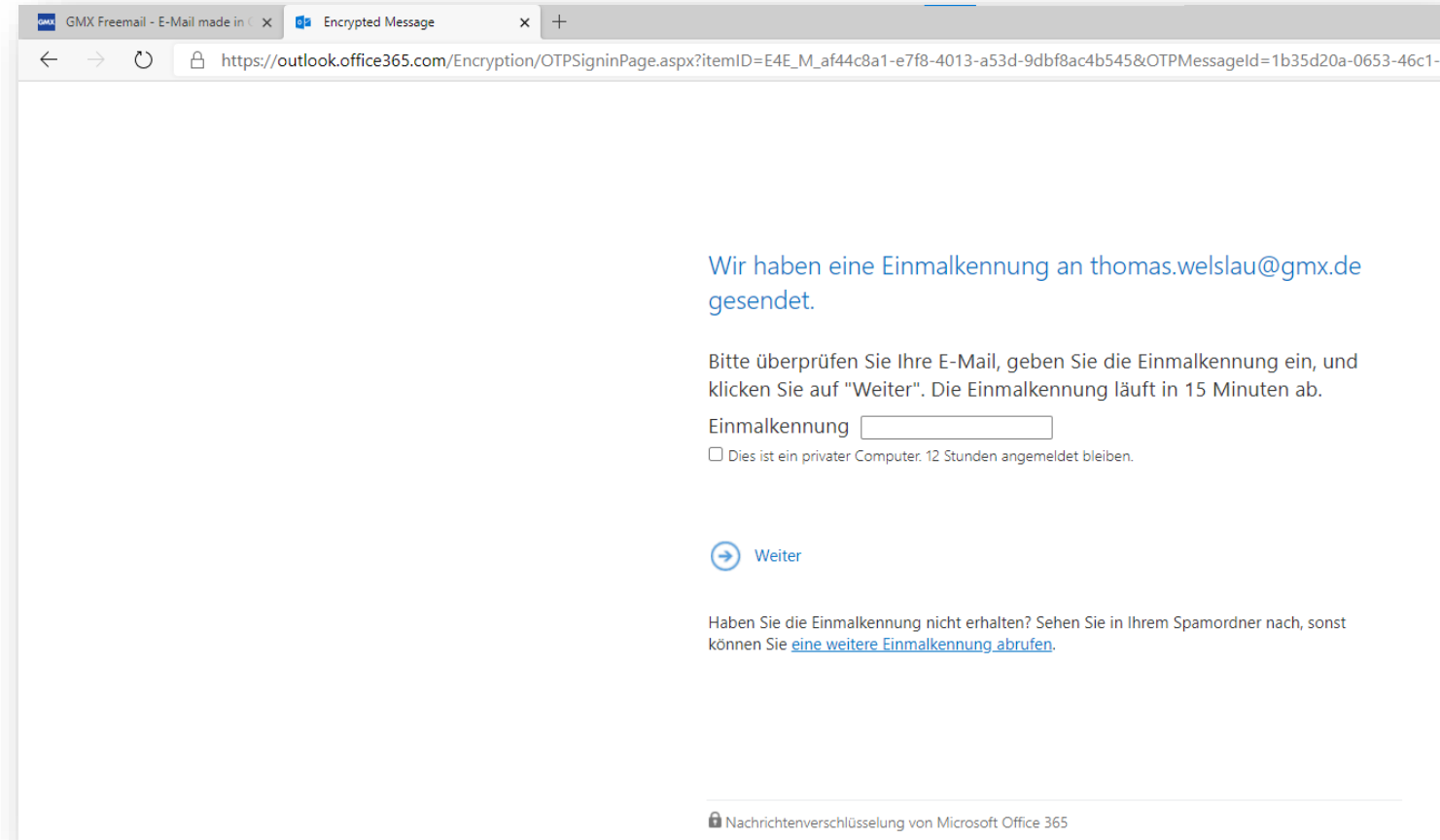
Anzeige der verschlüsselten
E-Mail im externen Mail Client
wie z.B. GMX



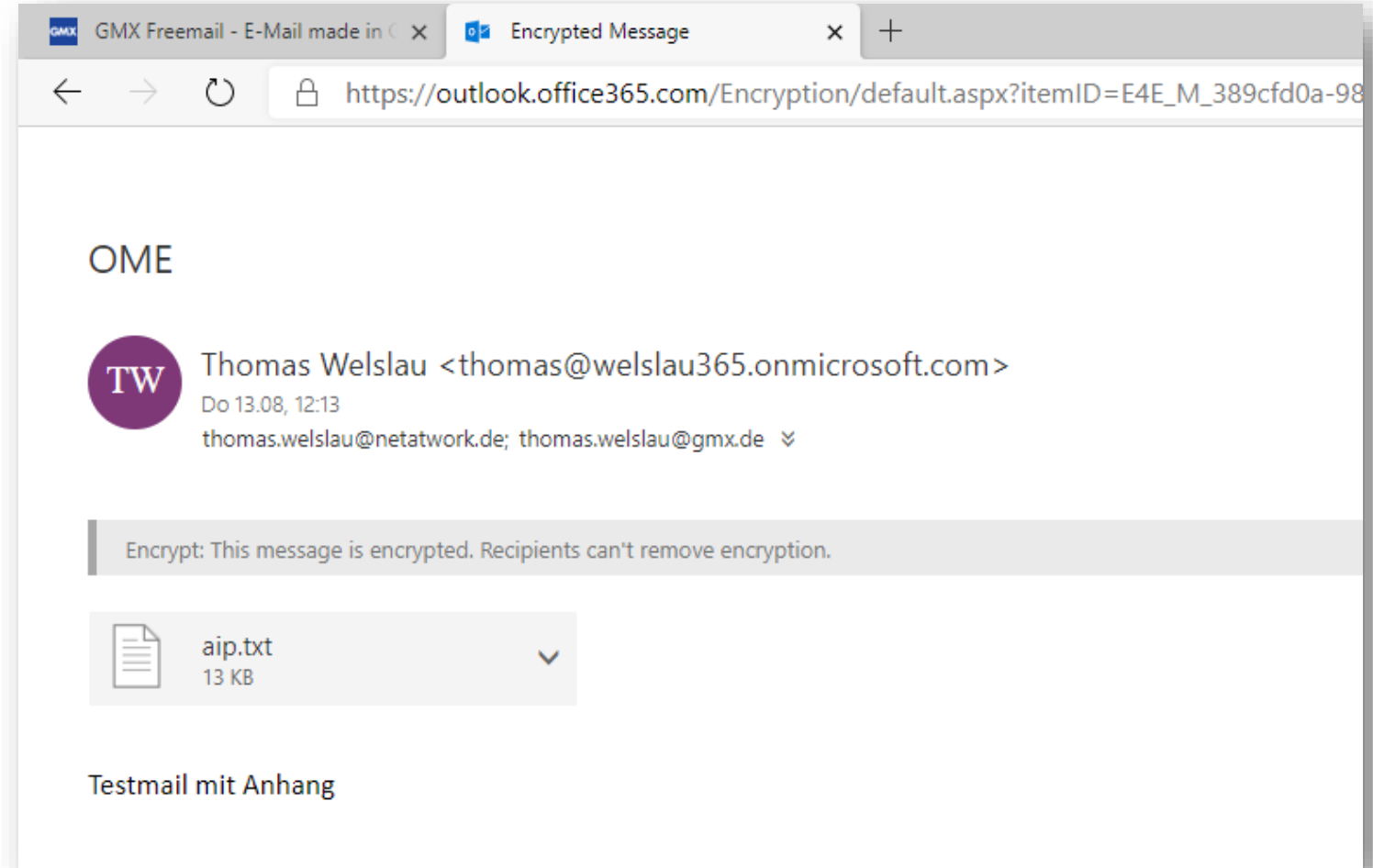
Verbindung zu Office 365 zum
Anzeigen der verschlüsselten
E-Mail



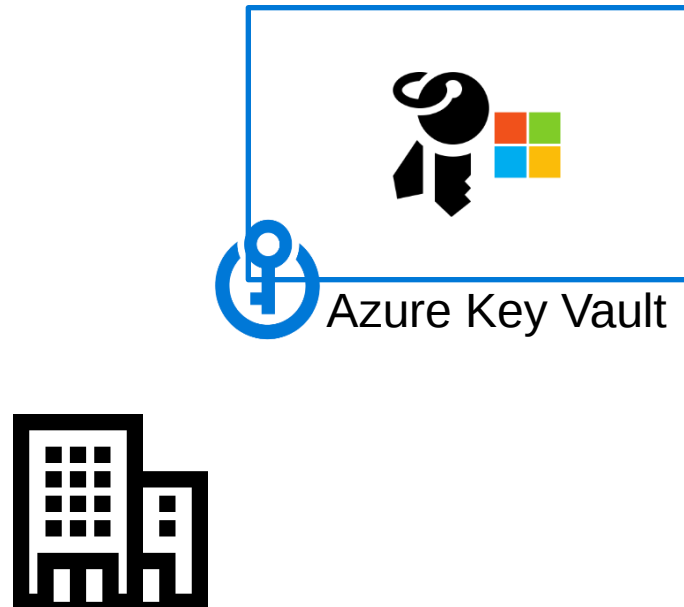
Zum Entschlüsseln wird eine Authentifizierung benötigt, hier ein Einmalkennwort



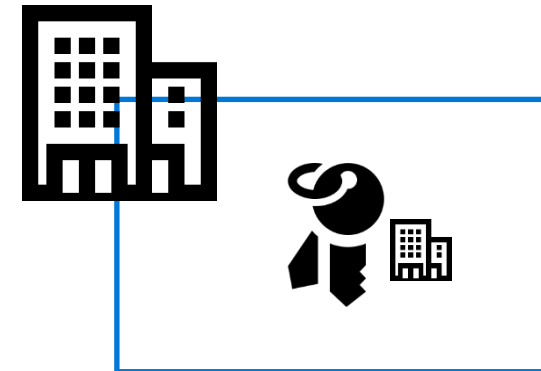
Anzeige der verschlüsselten E-Mail nach Authentifizierung



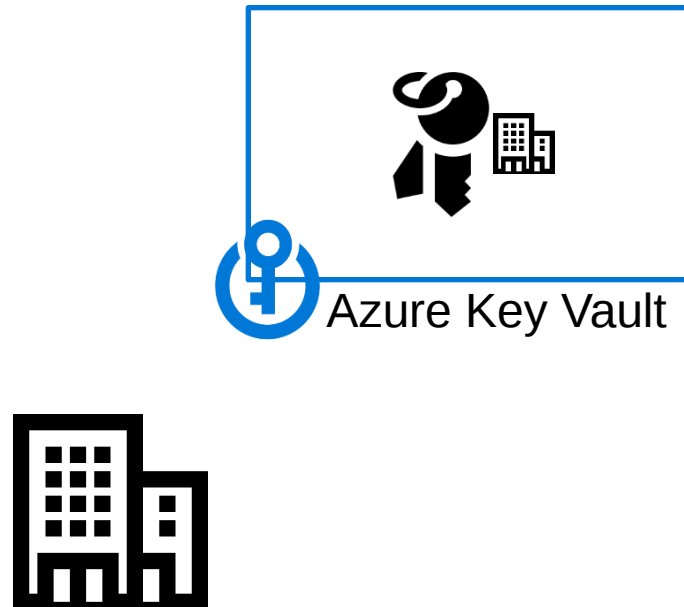
Microsoft verwalteter Schlüssel



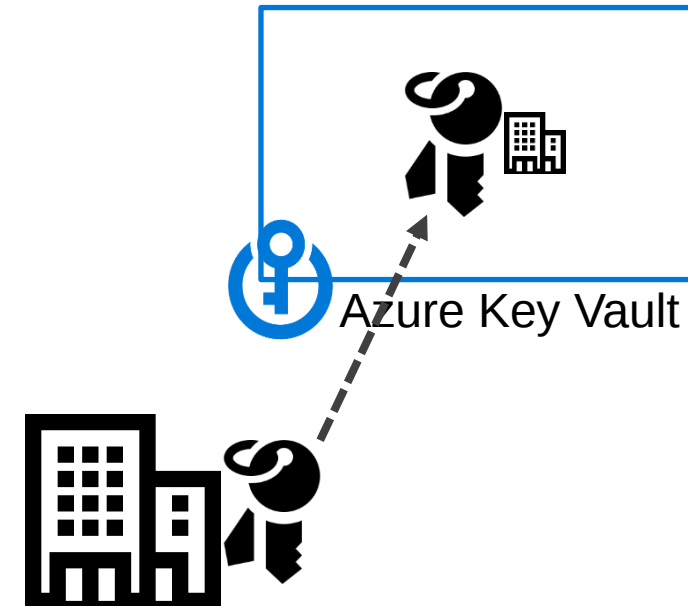
Hold your own key (HYOK)



Create your own key (CYOK)



Bring your own key (BYOK)



Double Key Encryption (DKE)

- Ein Schlüssel wird von Microsoft verwaltet und ein zusätzlicher Schlüssel liegt beim Kunden
- Für die Ver- und Entschlüsselung werden beide Schlüssel benötigt
- Umsetzung:
 - Lokale Bereitstellung des Dienstes
 - Generierung von privatem und öffentlichem Schlüssel
 - Veröffentlichung des Dienstes

Verschlüsselung
Kontrollieren, wer auf Dateien und E-Mails zugreifen kann, auf die diese Bezeichnung angewendet ist. [Weitere Informationen zu Verschlüsselungseinstellungen](#)

Verschlüsselung
Anwenden

ⓘ Die Aktivierung der Verschlüsselung wirkt sich auf Office-Dateien (Word, PowerPoint, Excel) aus, auf die diese Bezeichnung angewendet ist. Da die Dateien aus Sicherheitsgründen verschlüsselt werden, wird die Leistung langsam sein, wenn Dateien geöffnet oder gespeichert werden, und einige SharePoint- und OneDrive-Funktionen werden eingeschränkt oder gar nicht verfügbar sein. [Weitere Informationen](#)

Berechtigungen jetzt zuweisen oder Benutzer entscheiden lassen?
Berechtigungen jetzt zuweisen
Die von Ihnen ausgewählten Verschlüsselungseinstellungen werden automatisch erzwingen, wenn die Bezeichnung auf E-Mails oder Office-Dateien angewendet wird.

Benutzerzugriff auf Inhalt läuft ab. ⓘ
Nie

Offlinezugriff zulassen ⓘ
Immer

Bestimmen Benutzern und Gruppen Berechtigungen erteilen * ⓘ
[Berechtigungen zuweisen](#)

Benutzer und Gruppen	Berechtigungen
☒ Doppelschlüsselverschlüsselung verwenden (Vorschau) ⓘ Die URL des Dienstes für die Verschlüsselung mit doppeltem Schlüssel	

TeleTrust-EBCA "PKI-Workshop" 2020

Berlin, 01.10.2020

"Streitgespräch: AIP vs. S/MIME - Obsolet oder doch eine sinnvolle Zusammenarbeit?"

Thomas Welslau, Net at Work

Sören Beiler, Net at Work