

#TeamsNation

Securing Microsoft 365 Data with service encryption

Thomas Stensitzki



Sponsored by



Microsoft Teams



Microsoft Tech Community

Thomas Stensitzki

Enterprise Consultant | Geschäftsführer
Granikos GmbH & Co. KG
MVP | MCT | MCT Regional Lead

Twitter [@Stensitzki](https://twitter.com/Stensitzki)

LinkedIn <https://linkedin.com/in/thomasstensitzki>

Blog <http://Blog.Granikos.eu>

YouTube <http://TechTalk.Granikos.eu>



Was wir nicht betrachten

Transportverschlüsselung

Zwischen Kunde und Rechenzentrum

Zwischen Servern und Rechenzentrum



Was wir nicht betrachten

Azure Service Verschlüsselungen

- Client-Side Encryption
 - Azure Disk Encryption
 - Azure Storage Service Encryption
 - Azure Blob Client-Side Encryption
 - Azure SQL Database Data-at-Rest Encryption
 - Cosmos DB Database Encryption
 - Data Lake Encryption
 - SMB Encryption over Azure Virtual Networks
- Server-Side Encryption
 - Service-Managed Keys
 - Customer-Managed Keys (Bring Your Own Key BYOK)

Was wir nicht betrachten

E-Mail-Verschlüsselungen

- Nachrichtenverschlüsselung mit S/MIME
- Office 365 Message Encryption (OME)
- Vertraulichkeitsbezeichnungen (Sensitivity Label)

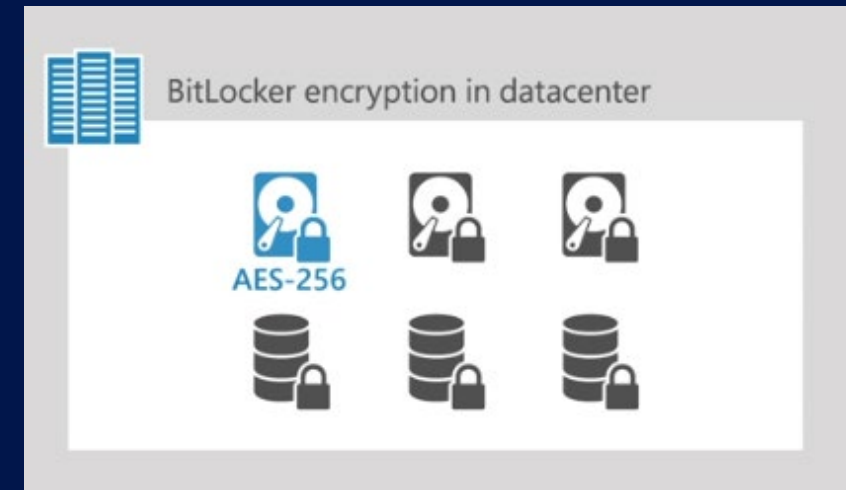
Verschlüsselung in Microsoft 365

Microsoft 365 Standard

- BitLocker → Dateisystem-Verschlüsselung in Microsoft Rechenzentren
- Shredded Storage → Verschlüsselung von Dateiteilen mit AES-256 Schlüsseln

Erweiterung der Standardverschlüsselung

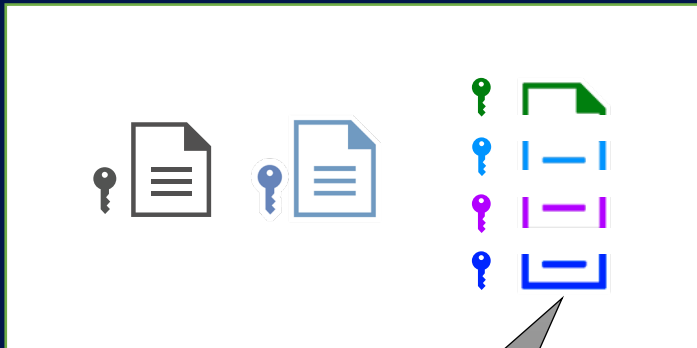
- Customer Managed KEY (CMK)
- Double Key Encryption (DKE)



SharePoint Online – Shredded Storage

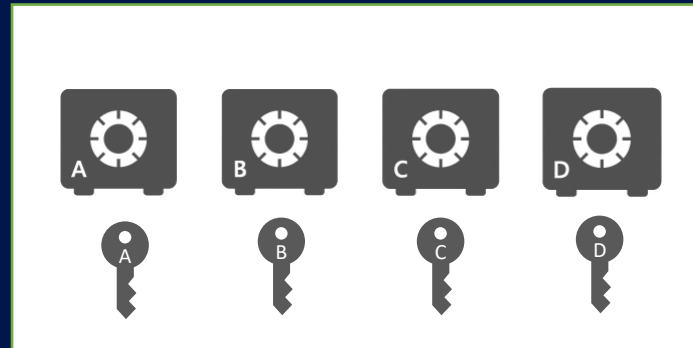
Encryption Data-at-Rest

Encrypted Files



Chunks

Azure Storage Containers



Key Store



Content Database



<https://aka.ms/dataencryption>

Customer Key



Sponsored by



Microsoft Teams



Microsoft Tech Community

Customer Key

Warum gibt es Customer Key in Microsoft 365?

- Verschlüsselung von Dateninhalten als zusätzliche Schutzebene zu BitLocker
- Trennung des Zugriffes für Windows Administratoren auf Applikationsdaten, die durch das Betriebssystem verarbeitet werden
- Customer Key Option ermöglicht eine Schlüsselverwaltung pro Mandant
- Ermöglicht die Umsetzung von besonderen Compliance-Anforderungen zur Verschlüsselung in Microsoft 365
- Schlüsselverwaltung durch den Kunden

Customer Key

Lizensierung

Feature Matrix

<https://m365maps.com>

Office 365 Enterprise ☐ E1 ☐ E3 ☒ E5
Microsoft 365 Business ☒ Basic ☒ Standard ☒ Premium
Microsoft 365 Frontline ☐ F1 ☐ F3 ☐ F5 Sec ☒ F5 Comp ☒ F5 Sec + Comp
Microsoft 365 Enterprise ☐ E3 ☐ E5 Sec ☒ E5 Comp ☒ E5
Microsoft 365 Education ☐ A1 (Legacy) ☐ A1 for Devices ☐ A3 ☐ A5 Sec ☒ A5 Comp ☒ A5
[Select All](#) / [Select None](#)

customer key	Office 365	Microsoft 365 Business			Microsoft 365 Frontline		Microsoft 365 Enterprise		Microsoft 365 Education	
Feature	E5	Basic	Standard	Premium	F5 Compliance	F5 Sec + Comp	E5 Compliance	E5	A5 Compliance	A5
Office 365	E5							E5		A5
Customer Key	✓				✓	✓	✓	✓	✓	✓

Administrator: Windows PowerShell

```
PS C:\SCRIPTS> (Get-Mailbox [redacted]).PersistedCapabilities
GRAPH_CONNECTORS_SEARCH_INDEX
CommunicationsCompliance
CustomerKey
M365Auditing
BPOS_S_InformationBarriers
BPOS_S_0365PremiumEncryption
BPOS_S_BookingsAddOn
MIP_S_CLP2
MYANALYTICSP2
BPOS_S_0365PAM
BPOS_S_Analytics
BPOS_S_ThreatIntelligenceAddOn
BPOS_S_FeminaAnalytics
```

Exchange Online
Management Shell



Customer Key

- Azure Key Vaults in zwei separaten Azure Abonnements → EA oder CSP
- Initiale Einrichtung der Customer Managed Keys über FastTrack Portal (Microsoft Empfehlung)
- Schlüsselungsmöglichkeiten
 - Allgemeine Microsoft 365 Data-at-Rest Verschlüsselung
 - Dienstverschlüsselung für Exchange Online und SharePoint Online (inkl. OneDrive und Microsoft Teams)
- Verwaltung
 - Erstellung von Data Encryption Policies (DEP)
 - Zuweisung von Data Encryption Policies
- Schlüsselwechsel
 - Rotation eines Customer Key
 - Rotation eines Availability Key → Keine direkte Kontrolle durch Endkunden

Weitere Informationen zum Schlüsselwechsel



Customer Key

Hinweise



- Löschen Sie keine Schlüssel, die mit DEP-Richtlinien verknüpft sind oder einmal aktiv verknüpft waren
- Inhalte werden bei einer Schlüsselrotation entschlüsselt und mit dem neuen Schlüssel erneut verschlüsselt
- Exchange Online
 - Aktive Postfächer werden regelmäßig neu verschlüsselt
 - Inaktive, deaktivierte und nicht mehr verbundene Postfächer können noch mit einem alten Schlüssel verschlüsselt sein
- SharePoint Online
 - Datensicherungen zur Wiederherstellung können Daten enthalten, die mit einem alten Schlüssel geschützt sind
- Risiko eines nachträglichen Datenverlustes

Customer Key

Schlüsselverwaltung

- On-Premises Hardware Service Module (HSM)
 - Empfehlung für den produktiven Einsatz
- Azure Key Vault (AKV)
 - Empfehlung für Testzwecke oder einen Proof-of-Concept
- Beide Varianten erfordern Azure Key Vaults für die Konfiguration und Verwaltung

Data Encryption Policies

Microsoft 365 Data-at-Rest für alle Anwender im Mandanten

- Teams Chat-Nachrichten (1:1 Chats, Gruppenchats, Meeting-Chats, Kanal-Konversationen)
- Teams Media-Nachrichten (Bilder, Code-Beispiele, Video-/Audio-Nachrichten, Wiki-Bilder)
- Teams Anruf- und Meeting-Aufzeichnungen in Teams-Speicherorten (aka Stream)
- Teams Chatbenachrichtigungen und Teams Chatempfehlungen von Cortana
- Teams Statusnachrichten
- Benutzer- und Signalinformationen in Exchange Online
- Exchange Online Postfächer, die nicht über eine dedizierte Postfach-DEP verschlüsselt sind
- Microsoft Information Protection
 - Exact Data Match (EDM) Daten
 - Label Vertraulichkeitskennzeichnungen (Sensitivity Label)
- Teams und EDM Daten werden ab Zuweisung der DEP-Richtlinie verschlüsselt
- Exchange Online Daten werden vollständig verschlüsselt



Data Encryption Policies

Microsoft 365 Data-at-Rest für alle Anwender im Mandanten



Folgenden Daten werden mit einer M365 Data-at-Rest DEP nicht verschlüsselt

- SharePoint Online und OneDrive for Business
 - Teams Dateien und Aufzeichnungen in SharePoint Online und OneDrive for Business
 - Teams Live Event Daten
 - Andere Microsoft 365 Daten, z.B. Yammer oder Planner
-
- Es können mehrere DEP für Microsoft 365 Data-at-Rest im Mandanten existieren
 - Nur eine DEP ist zugewiesen und aktiv

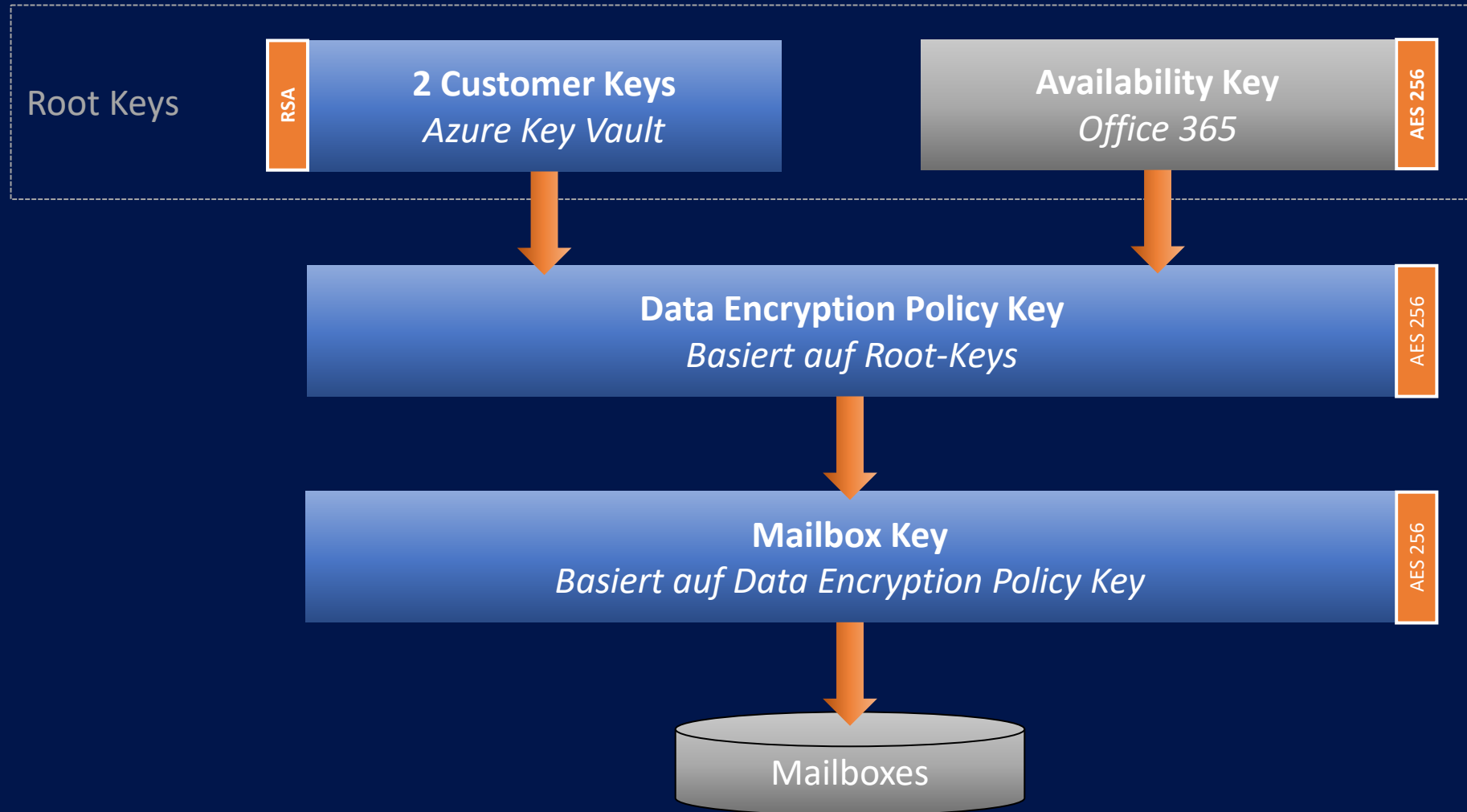
Data Encryption Policies

Exchange Online

- Verschlüsselung von unterschiedlichen Objekttypen
 - Benutzerpostfächern (Mailbox User)
 - E-Mail-Benutzer (Mail User)
 - Microsoft 365 Gruppen
 - Geteilte Postfächer
 - Öffentliche Ordner
- Je Postfach kann eine DEP zugewiesen werden
- Es können bis zu 50 aktive DEP im Mandanten existieren

Data Encryption Policies

Customer Key – Exchange Online und Microsoft Teams (Skype for Business)



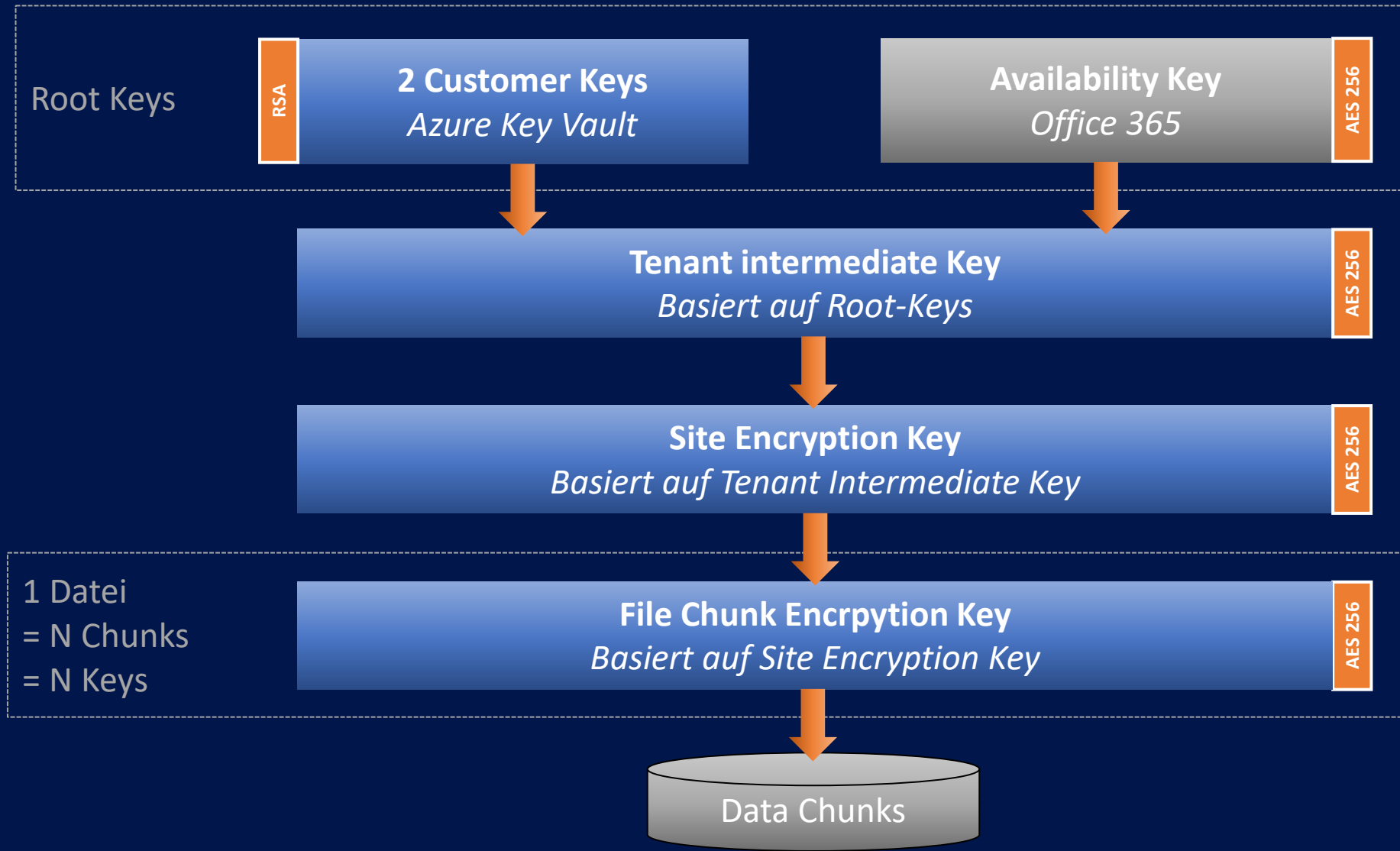
Data Encryption Policies

SharePoint Online, OneDrive for Business, Teams-Dateien

- Verschlüsselung von existierenden Daten beginnt unmittelbar nach Zuweisung der Schlüssel
- Verschlüsselung von Daten mit unterschiedlichen Schlüssel je Geo-Lokation möglich

Data Encryption Policies

Customer Key – SharePoint Online, OneDrive for Business, Teams-Dateien



Customer Key Implementierung



Sponsored by



Microsoft Teams



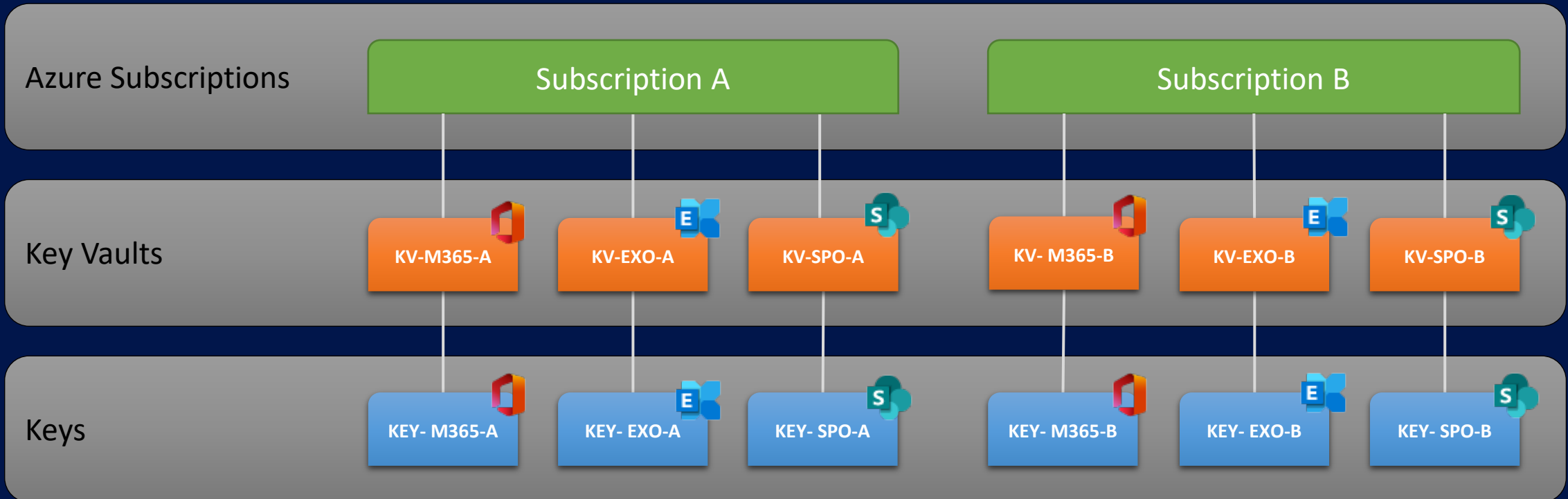
Microsoft Tech Community

Customer Key

Azure Abonnements und Key Vaults

Vor einer FastTrack-Anfrage zur Einrichtung von Customer Key im Microsoft 365 Mandanten

- Einrichtung von Azure Key Vaults und Keys in zwei Azure Abonnements
- Ein Key Vault mit Key für jeden zu verschlüsselnden Workload

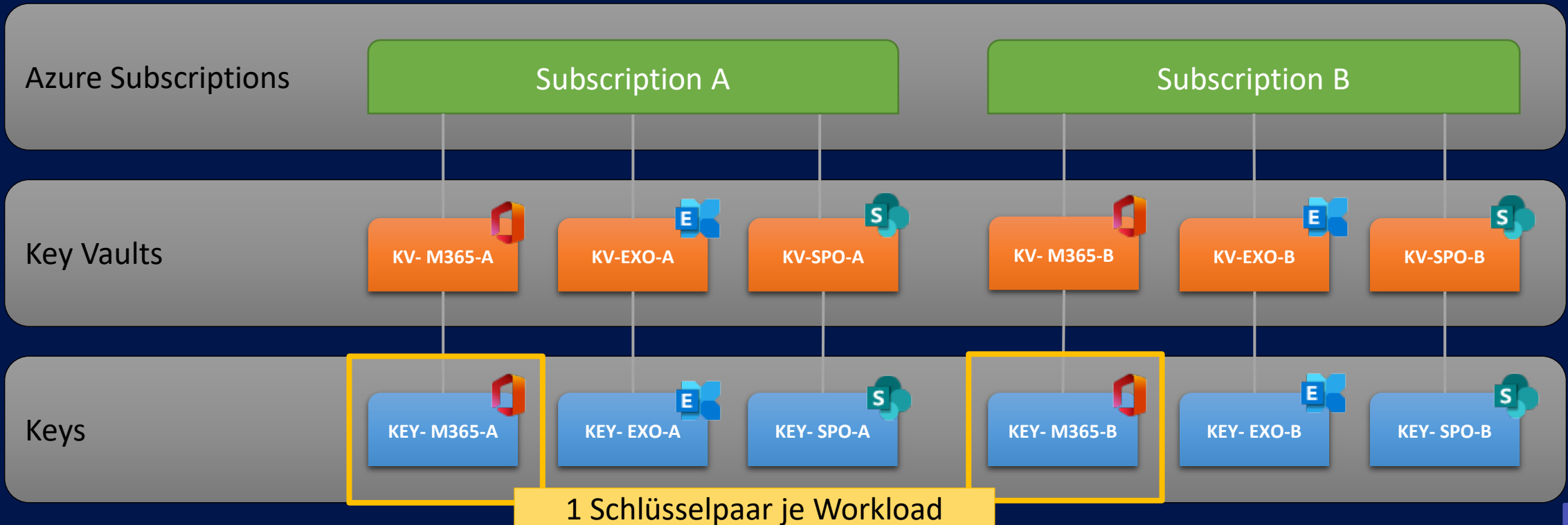


Customer Key

Azure Abonnements und Key Vaults

Vor einer FastTrack-Anfrage zur Einrichtung von Customer Key

- Einrichtung von Azure Key Vaults und Keys in zwei Azure Abonnements
- Ein Key Vault mit Key für jeden zu verschlüsselnden Workload



Customer Key

Einrichtung

1. Erstellung von Azure AD Sicherheitsgruppe für Administratoren
 - Administrator + Contributor
2. Erstellung von zwei Azure Abonnements
 - Trennung der Berechtigungen für Azure Ressourcengruppen, Key Vaults und Keys
 - AZ-EGXDE-CMK-A
 - AZ-EGXDE-CMK-B
3. Registrierung des Mandanten für Customer Key via FastTrack
4. Erstellung einer Ressourcengruppe in jedem Abonnement
5. Erstellung der benötigten Key Vaults in jeder Ressourcengruppe
 - Standard (Test, Proof-of-Concept) oder Premium (Produktiv)
6. Konfiguration der Zugriffsberechtigungen je Key Vault für Azure AD Sicherheitsgruppen
7. Erstellung der Keys je Key Vault

Key Vault und Key Namen sind global eindeutig



Customer Key

Einrichtung – Azure Context

```
Windows PowerShell

PS C:\SCRIPTS> Connect-AzAccount
WARNUNG: TenantId 'd320e379-89d3-4566-b834-6ca78a2f6399' contains more than one active subscription. First one will be
selected for further use. To select another subscription, use Set-AzContext.

Account                SubscriptionName TenantId                Environment
-----
admin@egxde.onmicrosoft.com AZ-EGXDE-CMK-B    d320e379-89d3-4566-b834-6ca78a2f6399 AzureCloud

PS C:\SCRIPTS> Get-AzSubscription


Name                Id                TenantId                State
----                -
AZ-EGXDE-CMK-B     efb2c208-5616-4d83-aae2-6b0ec6ee2108 d320e379-89d3-4566-b834-6ca78a2f6399 Enabled
AZ-EGXDE-1         f9ee38a2-1576-48b1-9ca9-7a2d62d11d53 d320e379-89d3-4566-b834-6ca78a2f6399 Enabled
AZ-EGXDE-CMK-A     59fc4549-dcc1-4c8d-bedd-4c7c7849af7c d320e379-89d3-4566-b834-6ca78a2f6399 Enabled

PS C:\SCRIPTS> Set-AzContext -SubscriptionId 59fc4549-dcc1-4c8d-bedd-4c7c7849af7c

Name                Account                SubscriptionName Environment                TenantId
----                -
AZ-EGXDE-CMK-A     (59fc4549-dcc1-4c8d-be... admin@egxde.onmi... AZ-EGXDE-CMK-A            AzureCloud                d320e379-89d3-4...
```


Customer Key

FastTrack

FastTrack

Microsoft 365 ▾ Azure Dynamics 365 Ressourcen ▾

Alles von Microsoft ▾

FastTrack – reibungslos und sicher in die Cloud umsteigen


Anmelden

Zur Anmeldung benötigen Sie ein Arbeits-, Schul- oder Unikonto. [Hilfe anfordern](#) >

Wenn Sie Behördenkunde sind und Unterstützung bei der Anmeldung benötigen, [erhalten Sie hier Hilfe](#).

<https://fasttrack.microsoft.com>

FastTrack erleichtert Kunden die Bereitstellung von Microsoft 365, Azure oder Dynamics 365 Abonnements ohne Zusatzkosten.

Microsoft

admin@setebos-ag.com

Permissions requested

FastTrack

[App info](#)

This app would like to:

- ✓ View your basic profile
- ✓ Maintain access to data you have given it access to

☐ Consent on behalf of your organization

Accepting these permissions means that you allow this app to use your data as specified in their [terms of service](#) and [privacy statement](#). You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

Cancel

Accept

Customer Key

FastTrack

Microsoft FastTrack-Registrierung

Vorname *

SAG

Nachname *

Administrator

E-Mail *

admin@setebos-ag.com

Alternative E-Mail-Adresse (optional)

Telefonnummer *

+49 123 45678

Telefondurchwahl (optional)

Land/Region *

Deutschland

Firmenname *

Setebos-AG

Der Name des Unternehmens kann zu einem späteren Zeitpunkt mit dem tatsächlichen Unternehmensnamen für diesen Tenant überschrieben werden.

Benutzertyp: *

- ☐ Microsoft-Partner - Ein Unternehmen mit gültiger Microsoft Partner Network ID (MPNID), das zu Microsoft-Lösungen berät oder diese bereitstellt, verwaltet, hostet, wiederverkauft oder vertreibt.
- ☒ Microsoft-Kunde - Eine Organisation, die Microsoft-Lösungen erworben hat und für Einrichtung, Migration oder technische Aspekte Unterstützung durch das FastTrack Center benötigt.

Titel *

IT-Administrator

Wichtiger Hinweis

FastTrack-Dienste stehen für anspruchsberechtigte Kunden zur Verfügung und werden durch Mitarbeiter von Microsoft bzw. durch von Microsoft genehmigte Lieferanten oder Partner ("FastTrack-Spezialisten") erbracht. FastTrack-Dienste sind "professionelle Dienstleistungen" und unterliegen dem entsprechenden Hinweis in den [Onlinedienstbedingungen](#). Eine vollständige Auflistung der Daten, die von den FastTrack-Diensten gesammelt werden, sowie der Art und Weise, wie Microsoft diese Daten nutzt, finden Sie in den [Datenschutzbestimmungen von Microsoft](#) und in der [FastTrack-Offenlegung](#).

☐ Ja, Microsoft kann mich nach Feedback zu meinen Erfahrungen mit FastTrack-Diensten fragen.

Mit Ihrer Registrierung bei FastTrack bestätigen Sie, dass Sie die Dienst- und Datenbedingungen von FastTrack gelesen und verstanden haben.


Abbrechen

Speichern



Customer Key


FastTrack

FastTrack Planung Bereitstellung Migration Einführen Ressourcen Hilfe 😊 🔔 SAG Administrator 👤 ▼

[FastTrack](#) / [Bereitstellung](#)

Bereitstellung

Fordern Sie Onboarding-Unterstützung mit individueller Remote-Hilfe unserer FastTrack Engineers an. Neben der Analyse Ihrer technischen Umgebung arbeiten sie mit Ihren IT-Mitarbeitern oder Partnern zusammen, um Sie beim Umstieg auf die Cloud zu unterstützen.




Leitfaden

[Microsoft 365-Bereitstellungszentrum besuchen](#)

[Weitere Informationen über Microsoft 365-Bereitstellungsberater](#)

[Leitfaden zum Anfordern von FastTrack-Unterstützung](#)

[Alle Bereitstellungsleitfäden anzeigen](#)




Unterstützung bei Microsoft 365 anfragen

[Berechtigte](#) Kunden können Unterstützung bei der Einrichtung (Onboarding) ihres Microsoft 365-Abonnements anfordern.

Erfahren Sie, wie Sie Unterstützung von FastTrack anfordern können.

[Unterstützung bei Microsoft 365 anfragen](#)




App Assure

Es werden Dienste zur Anwendungskompatibilität und zur Korrektur von Kompatibilitätsproblemen mit zulässigen Apps bei der Migration zu Windows 10, Windows Virtual Desktop (WVD), dem neuen Microsoft Edge und Microsoft 365 Apps (zuvor Office 365 ProPlus genannt) erbracht.

[Weitere Informationen zum App Assure-Dienst](#)


[Dienste zur Anwendungskompatibilität und Fehlerkorrektur anfordern](#)



Kundenschlüssel für SharePoint und OneDrive for Business

Office 365-Kunden erhalten die Möglichkeit, kundeneigene und kundenverwaltete Verschlüsselungsschlüssel mit SharePoint und OneDrive for Business zu verwenden.


[Verschlüsselungsschlüssel für SharePoint und OneDrive anfordern](#)



Kundenschlüssel für Exchange

Office 365-Kunden erhalten die Möglichkeit, kundeneigene und kundenverwaltete Verschlüsselungsschlüssel mit Exchange Online zu verwenden.

[Verschlüsselungsschlüssel für Exchange online anfordern](#)





Kundenschlüssel für Microsoft 365

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

[Hilfe zum Microsoft 365-Kundenschlüssel anfordern](#)

[Mehr anzeigen](#)



Customer Key

FastTrack

To begin Customer Key onboarding, please provide all the information requested in the table below:

Full Company Name	
Azure Subscription offer type i.e. Enterprise Agreement or via Cloud Service Provider (note: Pay As You Go, Free Trail, Azure Pass or Introductory Special are not eligible for Customer Key)	
Are you requesting Customer Key for Microsoft 365 i.e. multi-workload DEP?	Yes / No
FastTrack request ID for Customer Key for Microsoft 365	
Are you requesting Customer Key for Exchange?	Yes / No
FastTrack request ID for Customer Key for Exchange	
Are you requesting Customer Key for SharePoint and OneDrive for Business?	Yes / No
FastTrack request ID for SharePoint and OneDrive for Business	
Is this a multi-geo tenant? (Information only required if onboarding SharePoint/OneDrive-for-Business) If yes, please provide the Tenant FQDNs and subscription IDs for all the Geos	Geo1: Geo2: Geo3: Geo4:
Two customer contacts in charge of Customer Key onboarding for the tenant. These individuals will be contacted by Microsoft in case there any issues in onboarding the tenant.	Contact 1 <ul style="list-style-type: none"> Name: Email: Phone: Contact 2 <ul style="list-style-type: none"> Name: Email: Phone:
Your Microsoft Sales Account Team contacts	Contact 1 <ul style="list-style-type: none"> Name: Email: Contact 2 <ul style="list-style-type: none"> Name: Email:
Azure Subscription IDs where Azure Key Vaults for storing keys for M365DataAtRestEncryption are to be located. Requires Two.	Subscription ID #1: Subscription ID #2:
Azure Subscription IDs where Azure Key Vaults for storing keys for Exchange are to be located. Requires Two.	Subscription ID #1: Subscription ID #2:
Azure Subscription IDs where Key Vaults for storing keys for SharePoint/OneDrive-for-Business are to be located. Requires Two.	Subscription ID #1: Subscription ID #2:
The FQDN of the tenant to be onboarded to Customer Key: xxxxxxxxx.onmicrosoft.com	
Has this tenant onboarded to Customer Key Encryption before? If so, what was onboarded, Exchange or SharePoint?	



Customer Key

Einrichtung – Azure Funktionen und Ressourcengruppe je Subscription

```
# Registrierung des Provider Feature MandatoryRetentionPeriod
```

```
# Verhindert ein versehentliche Löschung des Azure Abonnements
```

```
Register-AzProviderFeature -FeatureName mandatoryRetentionPeriodEnabled -ProviderNamespace  
Microsoft.Resources
```

```
# Registrierung
```

```
Register-AzResourceProvider -ProviderNamespace Microsoft.KeyVault
```

```
# Einrichtung der Ressourcengruppe für Azure Key Vaults
```

```
New-AzResourceGroup -Name RG-EGXDE-KV-A -Location "West Europe"
```

Abfrage der Azure Lokationen
Get-AzLocation

```
# Einrichtung des ersten Key Vaults per Azure Portal
```

```
# Speichern der Vorlagen- und Parameterdatei für die weiteren Key Vaults
```



Customer Key

Einrichtung – Einrichtung Key Vault

Vorbereitung der Parameterdatei

```
"parameters": {  
    "name": {  
        "value": "az-kv-egxde-exo-a"  
    }  
    {...}  
"accessPolicies": {  
    "value": [  
        {  
            "objectId": "754e1dbe-1bcf-4789-bbee-22410877fdb0",  
            "tenantId": "d320e379-89d3-4566-b834-6ca78a2f6399",  
            "permissions": {  
                "keys": {  
                    "create": true,  
                    "delete": true,  
                    "encrypt": true,  
                    "get": true,  
                    "import": true,  
                    "list": true,  
                    "manage": true,  
                    "recover": true,  
                    "restore": true,  
                    "sign": true,  
                    "unprotect": true,  
                    "update": true,  
                    "verify": true  
                }  
            }  
        }  
    ]  
}
```

Key Vault Namen sind global eindeutig

Template-Datei laden und in Json konvertieren

```
$TemplateFile = [System.IO.File]::ReadAllText("C:\CMK\keyvault-template.json")  
$TemplateJson = ConvertFrom-Json $TemplateFile -AsHashtable
```

Neue Ressourcengruppe erstellen

```
New-AzResourceGroupDeployment -ResourceGroupName "RG-EGXDE-KV-A" -TemplateObject ` $TemplateJson -TemplateParameterFile "C:\CMK\keyvault-parameters-exo-a.json"
```

Customer Key

Einrichtung – Konfiguration der Zugriffsberechtigungen je Key Vault – Teil 1

```
# Variablen für Key Vault und Admin Sicherheitsgruppe
```

```
$kvName = 'az-kv-egxde-exo-a'
```

```
$kvAdminGroup = 'kv-Admins'
```

```
# Setzen der Zugriffsrichtlinie für Administratoren
```

```
Set-AzKeyVaultAccessPolicy -VaultName $kvName `
```

```
-ObjectId (Get-AzADGroup -SearchString $kvAdminGroup)[0].Id `
```

```
-PermissionsToKeys create,import,list,get,backup,restore
```

```
# Konfiguration der Contributor-Gruppe via Azure Portal für die Ressourcengruppe
```

Customer Key

Einrichtung – Konfiguration der Zugriffsberechtigungen je Key Vault – Teil 1

Microsoft Azure

Search resources, services, and docs (G+/I)

admin@egxde.onmicro...
EAGLEWORX (EGXDE.ONMICROS...

Home > Subscriptions > AZ-EGXDE-CMK-A

AZ-EGXDE-CMK-A | Access control (IAM)

Subscription

Search (Ctrl+/)

+ Add Download role assignments Edit columns Refresh Remove Got feedback?

Check access **Role assignments** Roles Deny assignments Classic administrators

Number of role assignments for this subscription ⓘ
3 2000

Search by name or email Type: All Role: All Scope: All scopes Group by: Role

3 items (1 Users, 1 Groups, 1 Foreign Principals)

<input type="checkbox"/> Name	Type	Role	Scope	Condition
▼ Contributor				
<input type="checkbox"/> kv-Contributors	Group	Contributor ⓘ	This resource	None
▼ Owner				
<input type="checkbox"/> Foreign Principal for 'ALSO Germany CSP' in f	Foreign principal	Owner ⓘ	This resource	None
<input type="checkbox"/> Rick Blaine (ADM) admin@egxde.onmicrosoft.com	User	Owner ⓘ	This resource	None

Customer Key

Einrichtung – Konfiguration der Zugriffsberechtigungen je Key Vault – Teil 2

Variablen für Key Vault

```
$kvName = 'az-kv-egxde-exo-a'
```

Microsoft 365 Workloads

```
$objExoSfB = '00000002-0000-0ff1-ce00-000000000000'
```

```
$objSpoTeams = '00000003-0000-0ff1-ce00-000000000000'
```

```
$objMultiWL = 'c066d759-24ae-40e7-a56f-027002b5d3e4'
```

Exchange Online / Skype for Business

```
Set-AzKeyVaultAccessPolicy -VaultName $kvName -PermissionsToKeys wrapKey,unwrapKey,get `
-ServicePrincipalName $objExoSfB
```

SharePoint Online / OneDrive for Business / Teams Files

```
Set-AzKeyVaultAccessPolicy -VaultName $kvName -PermissionsToKeys wrapKey,unwrapKey,get `
-ServicePrincipalName $objSpoTeams
```

Microsoft 365 Multi-Workload

```
Set-AzKeyVaultAccessPolicy -VaultName $kvName -PermissionsToKeys wrapKey,unwrapKey,get `
-ServicePrincipalName $objMultiWL
```



Customer Key

Einrichtung – Erstellung der Azure Key Vault Keys

Variablen für Key Vault

```
$kvName = 'az-kv-egxde-exo-a'
```

Exchange Online / Skype for Business

```
Add-AzKeyVaultKey -VaultName $kvName -Name 'egxde-exo-key-a' -Destination 'Software'
```

SharePoint Online / OneDrive for Business / Teams Files

```
Add-AzKeyVaultKey -VaultName $kvName -Name 'egxde-spo-key-a' -Destination 'Software'
```

Microsoft 365 Multi-Workload

```
Add-AzKeyVaultKey -VaultName $kvName -Name 'egxde-m365dr-key-a' -Destination 'Software'
```

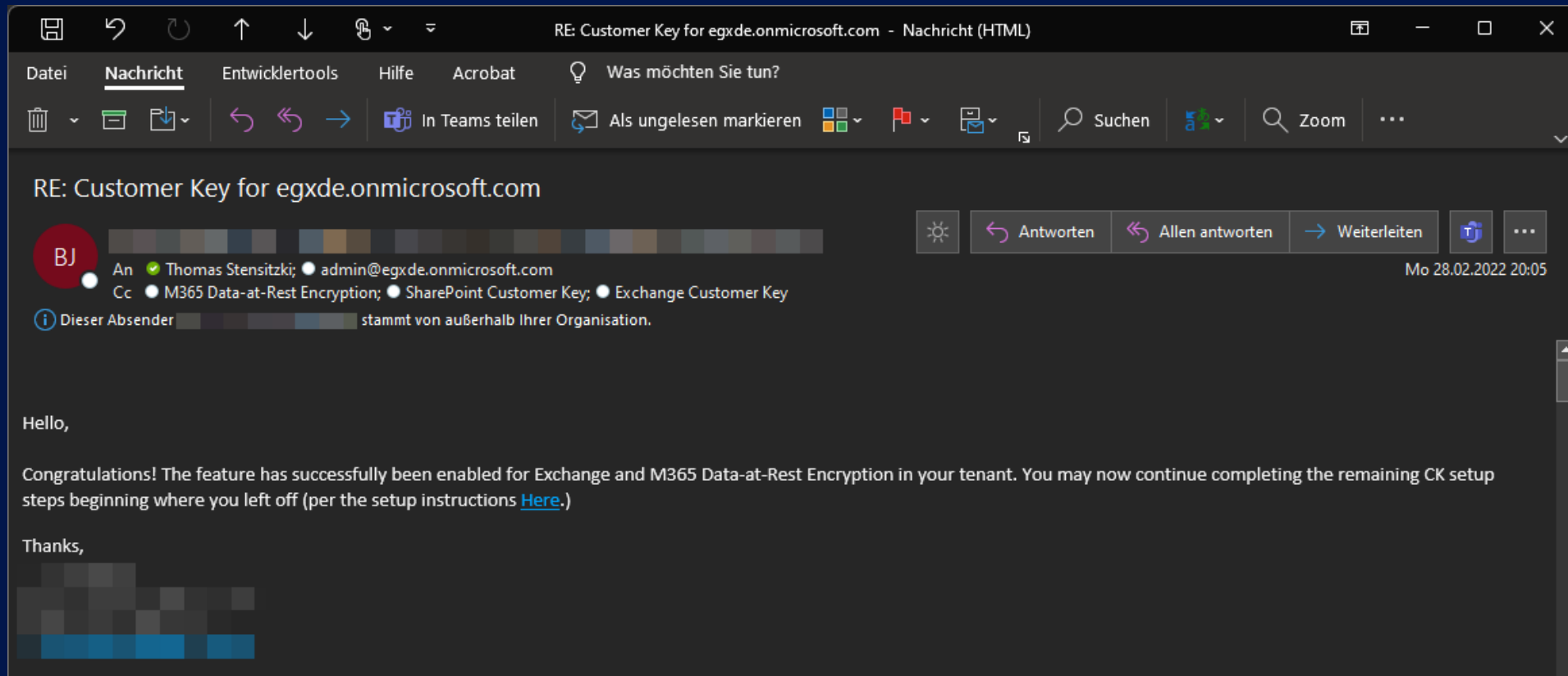
Key Namen sind global eindeutig



Customer Key

FastTrack Prozess

- Meldung an FastTrack per E-Mail



Data Encryption Policies

Customer Key – Microsoft 365 Multi-Workload

```
# PowerShell Modul: ExchangeOnlineManagement
```

```
Connect-ExchangeOnline
```

```
# Variablen
```

```
$key1 = 'https://az-kv-egxde-m365dr-a.vault.azure.net:443/keys/egxde-m365dr-key-a'
```

```
$key2 = 'https://az-kv-egxde-m365dr-b.vault.azure.net:443/keys/egxde-m365dr-key-b'
```

```
# Erstellung der Multi-Workload Data Encryption Policy
```

```
New-M365DataAtRestEncryptionPolicy -Name 'EGX_DataAtRest' `
-AzureKeyIDs $key1,$key2 -Description 'EGX Data at Rest Multi-Workload policy'
```

```
# Setzen der Multi-Workload DEP
```

```
Set-M365DataAtRestEncryptionPolicyAssignment -DataEncryptionPolicy 'EGX_DataAtRest'
```



Data Encryption Policies

Customer Key – Microsoft 365 Multi-Workload

```
Get-M365DataAtRestEncryptionPolicyAssignment | fl
```

```
RunspaceId           : 1d83f812-f929-4eb3-bd5d-881184373ba1
OrgHierarchyToIgnore  :
IsDeleted             : False
Rdn                   : CN=EGX_DataAtRest
Parent                : egxde.onmicrosoft.com\CKaaS Data Encryption Policies
Depth                 : 8
DistinguishedName     : CN=EGX_DataAtRest,CN=CKaaS Data Encryption
Policies,CN=Configuration,CN=egxde.onmicrosoft.com,CN=ConfigurationUnits,DC=DEUP281A001,DC=PRO
D,DC=OUTLOOK,DC=COM
IsRelativeDn          : False
DomainId              : DEUP281A001.PROD.OUTLOOK.COM
PartitionGuid         : 59ce2f71-eaa2-4ddf-a4fa-f25069d0b324
PartitionFQDN         : DEUP281A001.PROD.OUTLOOK.COM
ObjectGuid            : 05a9e413-6822-4918-8d8c-99b1aba1e06c
Name                  : EGX_DataAtRest
SecurityIdentifierString :
```



Data Encryption Policies

Customer Key – Exchange Online

Variablen

```
$key1 = 'https://az-kv-egxde-exo-a.vault.azure.net:443/keys/egxde-exo-key-a'  
$key2 = 'https://az-kv-egxde-exo-b.vault.azure.net:443/keys/egxde-exo-key-b'
```

Erstellung der Exchange Online Data Encryption Policy

```
New-DataEncryptionPolicy -Name 'EGX_EXO_DEP' `  
-AzureKeyIDs $key1,$key2 `  
-Description 'EGX Exchange Online Encryption Policy'
```

Setzen der Exchange Online DEP

```
Set-Mailbox LouisR@varunagroup.de -DataEncryptionPolicy 'EGX_EXO_DEP'  
Set-Mailbox LouisR@varunagroup.de -DataEncryptionPolicy 'EGX_EXO_DEP' -PublicFolder
```

```
Set-MailUser OnPremUser@varunagroup.de -DataEncryptionPolicy 'EGX_EXO_DEP'
```

```
Set-UnifiedGroup SomeGroup@groups.varunagroup.de -DataEncryptionPolicy 'EGX_EXO_DEP'
```

Prüfung für Postfächer

```
Get-MailboxStatistics UPN | FL IsEncrypted
```



Data Encryption Policies

Customer Key – SharePoint Online

```
# PowerShell Modul: Microsoft.Online.SharePoint.PowerShell
Connect-SPOService -Url https://tenant-admin.sharepoint.com
```

Abfrage der Key Versionen

```
Set-AzContext -SubscriptionId SUBSCRIPTION-A
$key1version = (Get-AzKeyVaultKey -VaultName az-kv-egxde-spo-a -Name egxde-spo-key-a `
-IncludeVersions).Version
```

```
Set-AzContext -SubscriptionId SUBSCRIPTION-B
$key2version = (Get-AzKeyVaultKey -VaultName az-kv-egxde-spo-b -Name egxde-spo-key-b `
-IncludeVersions).Version
```

Erstellung der SharePoint Online Data Encryption Policy

```
Register-SPODataEncryptionPolicy -PrimaryKeyVaultName 'az-kv-egxde-spo-a' -PrimaryKeyName
'egxde-spo-key-a' -PrimaryKeyVersion $key1version -SecondaryKeyVaultName 'az-kv-egxde-spo-b' -
SecondaryKeyName 'egxde-spo-key-b' -SecondaryKeyVersion $key2version
```

Prüfung

```
Get-SPODataEncryptionPolicy
```



Double Key Encryption

Überblick

- Verschlüsselung einer Teilmenge von Microsoft 365 Daten
- Informationsschutz mit Vertraulichkeitsbezeichnungen (Sensitivity Label)
- Nutzung von HSM-Lösungen (z.B. Thales)
 - Kompilierung des DKE GitHub Repository
- Keine Unterstützung von
 - Transport Regeln, inkl. Anti-Malware- und Anti-Spam-Funktionen für Nachrichteninhalte
 - Microsoft Delve
 - eDiscovery
 - Inhaltssuche und Indizierung
 - Office Web Apps und Co-Authoring

Customer Key

Zusammenfassung

- Customer Key unterstützt drei Verschlüsselungsziele
 - Microsoft 365 Data-at-Rest
 - Exchange Online
 - SharePoint Online
- Nicht alle Microsoft 365 Workloads unterstützen Customer Key Verschlüsselung
- Customer Key erfordert eine Lizenzierung für jedes Benutzerkonto
- Customer Key benötigt mindestens zwei Azure Abonnements für Key Vaults
- Ein Key Vault für jedes gewünschte Verschlüsselungsziel
- Aktivierung von Customer Key über Microsoft FastTrack (Microsoft Empfehlung)
- Definition der Zugriffsberechtigungen für Azure Abonnements und Key Vault
- Umsetzung einer Test-Implementierung in einem Test-Mandanten

Rate my session & Calls to Action



Rate this
session

1



Attend more
sessions and
join our
keynotes at
19.00 CET

2



Show your love
on social using
#TeamsNation
and
@TeamsNation

3

[https://teamsnation.rocks/
feedback](https://teamsnation.rocks/feedback)

Ressourcen

Subtitle

[Understanding Microsoft Information Protection Encryption Key Types](#)

[Roll or rotate a Customer Key or an availability key](#)

[Move requests in the Microsoft 365 or Office 365 service](#)

[Encryption ciphers used by Customer Key](#)

[Encryption for Skype for Business, OneDrive for Business, SharePoint Online, Microsoft Teams, and](#)

[Exchange Online](#)

[Microsoft 365 Multi-Geo eDiscovery configuration](#)

[Microsoft 365 encryption technical reference](#)

[Assign roles in Azure Portal](#)

[Microsoft 365 Maps](#)

[Double Key Encryption](#)

