CryptoPanel

edycja #24

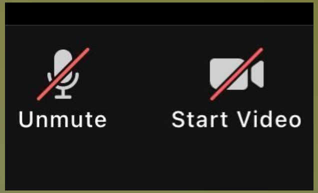
Już za moment zaczynamy...

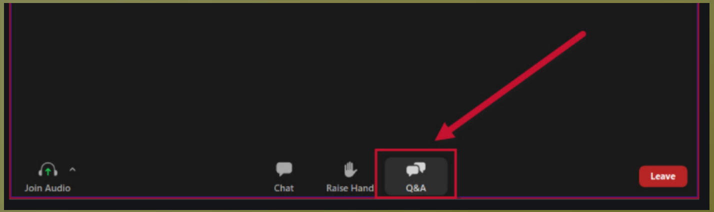
CryptoPanel

THALES

CLICO

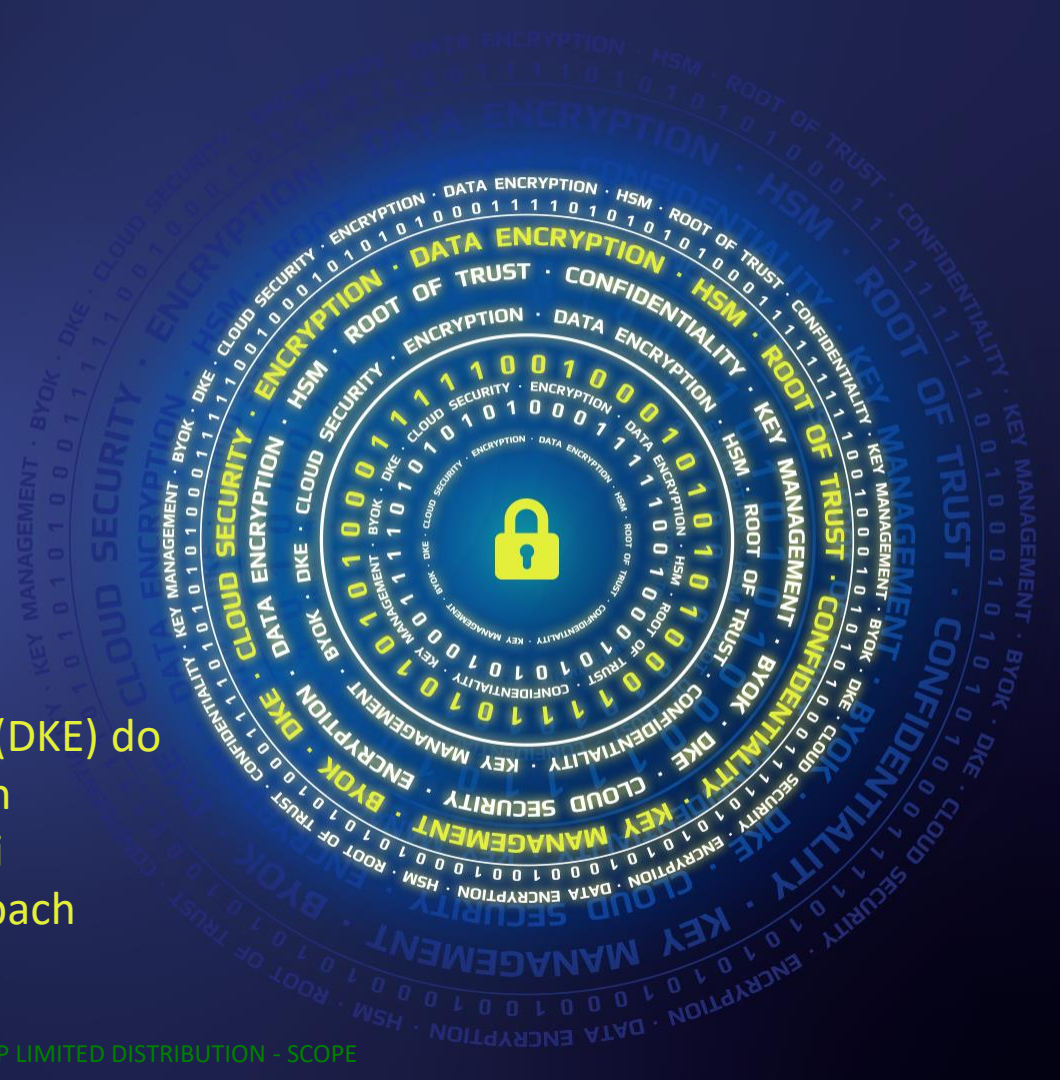
CryptoPanel





CryptoPanel

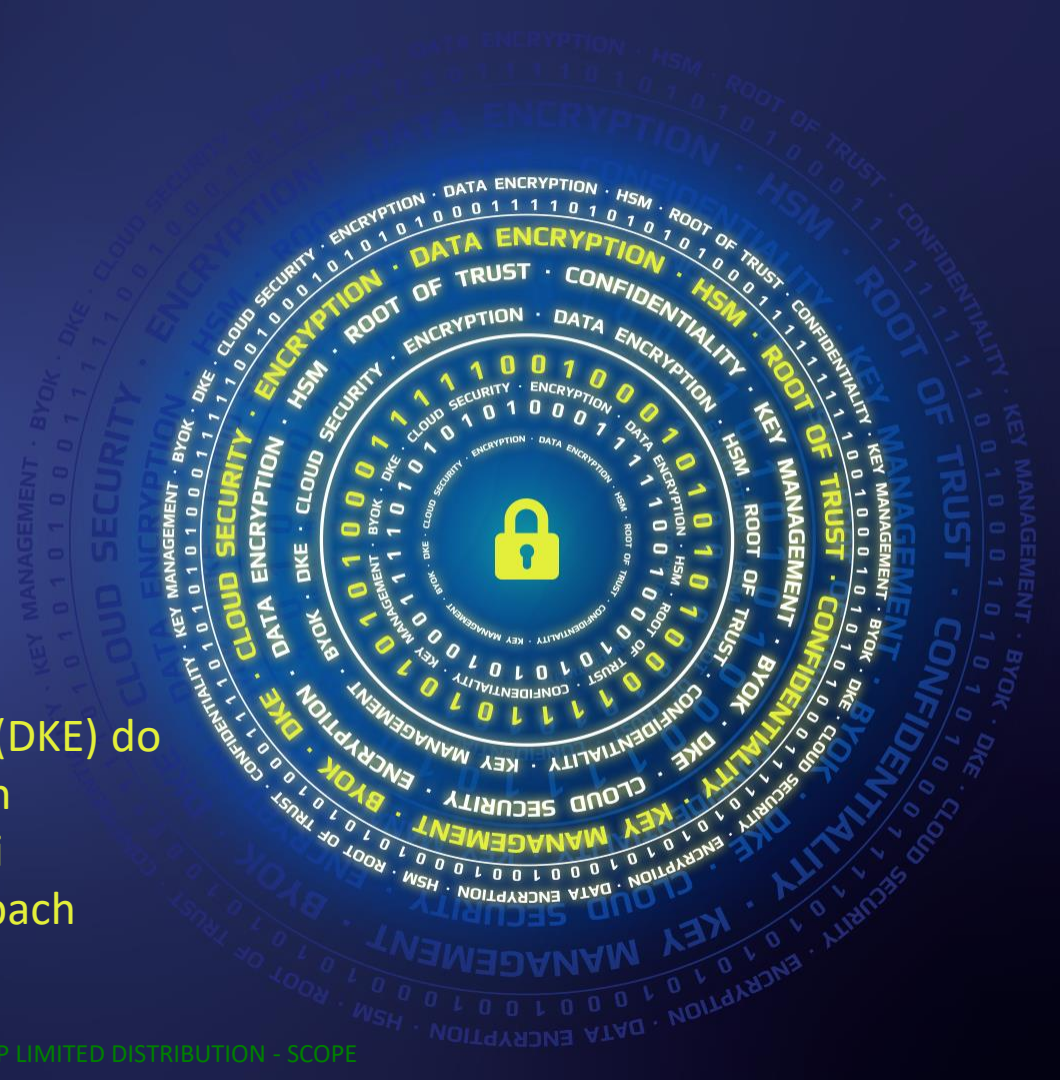
edycja #24



Jak wykorzystać podwójne szyfrowanie (DKE) do ochrony danych osobowych, kluczowych dokumentów firmowych oraz informacji finansowych przechowywanych w zasobach usługodawcy chmurowego.

CryptoPanel

TEST WIEDZY #24



Jak wykorzystać podwójne szyfrowanie (DKE) do ochrony danych osobowych, kluczowych dokumentów firmowych oraz informacji finansowych przechowywanych w zasobach usługodawcy chmurowego.


...AND
MICROSOFT
FOR ALL
CBS
SONY
CryptoPanel
edycja #7
...And Microsoft For All...
Bezpieczeństwo danych w Microsoft365 to przede wszystkim ich szyfrowanie.
Poprawna implementacja Double Key Encryption (DKE) - przykład strategii Hold Your Own Key (HYOK).
MS ADCA 5:00
MS SQL EKM 10:01
AZURE BYOK 21:05
W11 & TPM 22:30
O365 DKE (REMIX) 6:20
CDN... 3:20
ALL RIGHTS OF THE MANUFACTURER AND OF THE OWNER OF THE RECORDED WORK RESERVED UNAUTHORIZED PUBLIC PERFORMANCE, BROADCASTING AND COPYING OF THIS DISC PROHIBITED. CBS/SONY RECORDS, A DIVISION OF CBS/SONY

CryptoPanel

dziś dyskutują

Artur Holeczek

Partner Account Manager /
Product Manager
artur.holeczek@clico.pl
mob. +48 667 699 444

Jarosław Ulczok

Pre-sales Consultant
Jaroslaw.Ulczok@thalesgroup.com
mob. +48 603 056 667

CryptoPanel

problem

co nas boli...

- **Nasz jednostka korzystamy szeroko z rozwiązań firmy Microsoft:**
  - Microsoft 365
  - Azure, EntraID, …
- **Działamy na rynku silnie regulowanym (RODO, NIS2, itp)**
- **Przetwarzamy wiele dokumentów Office z czego ok. 5% dokumentów jest poufnych a 10% wrażliwych. Dla obu chcemy zapewnić poufność podczas przechowywaniu, przesyłu i użycia.**
- **Rozważamy użycie podwójnego szyfrowania w M365.**

- **Jakie mamy możliwości wdrożenia DKE dla zapewnić poufność dokumentów tworzonych w M365?**
- **Czy stosując DKE możemy wymieniać dokumenty chronione z innymi firmami?**
- **Czy warto zakupić *DKE Service (Key Broker)* dla obsługi DKE czy utrzymywać go samemu?**
- **Czy DKE nie stanie się wąskim gardłem w przypadku pracy wiele uosób nad wieloma dokumentami jednocześnie?**
- **Jak mogę wykorzystać DKE do ochrony zasobów Azure (serwery wirtualne, bazy danych, itp..)**

CryptoPanel

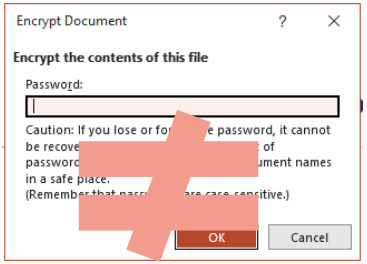
rozwiązanie

Kilka oczywistych oczywistości o DKE

Microsoft Double Key Encryption

DKE to odpowiedź M$ na zapotrzebowanie na HYOK w Azure. Działa tylko z wybranymi aplikacjami Office.

DKE to inne szyfrowanie dokumentów niż to wbudowane w aplikacje Office



Podwójne szyfrowanie kluczy (DKE)

Ochrona DKE zapewnia dodatkowe zabezpieczenia zawartości przy użyciu dwóch kluczy: jeden utworzony i przechowywany przez firmę Microsoft na platformie Azure, a drugi utworzony i przechowywany lokalnie przez klienta.

DKE wymaga, aby oba klucze miały dostęp do chronionej zawartości, zapewniając, że firma Microsoft i inne podmioty trzecie nigdy nie mają dostępu do chronionych danych samodzielnie.

Magazyn DKE można wdrożyć w chmurze lub lokalnie, zapewniając pełną elastyczność lokalizacji przechowywania.

Użyj DKE, gdy organizacja:

- Chce mieć pewność, że tylko oni mogą odszyfrować chronioną zawartość we wszystkich okolicznościach.
- Nie chcesz, aby firma Microsoft miała dostęp do chronionych danych samodzielnie.
- Ma wymagania prawne dotyczące przechowywania kluczy w granicach geograficznych. W przypadku DKE klucze przechowywane przez klienta są przechowywane w centrum danych klienta.

Uwaga

DKE jest podobna do skrzynki zabezpieczającej, która wymaga zarówno klucza bankowego, jak i klucza klienta w celu uzyskania dostępu. Ochrona DKE wymaga zarówno klucza przechowywanego przez firmę Microsoft, jak i klucza przechowywanego przez klienta w celu odszyfrowania chronionej zawartości.

Aby uzyskać więcej informacji, zobacz Podwójne szyfrowanie klucza w dokumentacji platformy Microsoft 365.

Źródło: https://learn.microsoft.com/pl-pl/azure/information-protection/plan-implement-tenant-key

Kiedy zdecydować się na DKE?

When your organization should adopt DKE

DKE isn't for every organization, nor for all of your data. Let's say a typical organizational data landscape has the following structure:

- Nonsensitive data (about 80% of data): Most of an organization's data falls into this category. There are no issues or concerns with moving this data to the cloud today. Moving such data to the cloud can be beneficial and the organization can use the security built into the cloud.
- Sensitive (about 15% of data): Sensitive data needs to be protected. The organization expects the cloud service provider to provide security while enhancing productivity for this category of data so that they can meet compliance regulations. You want to ensure this data is labeled correctly using Microsoft Purview Information Protection and is protected with access control and retention and audit policies.
- Highly sensitive (about 5% of data): This set is the organization's crown jewels and needs to be heavily guarded. The organization doesn't want anyone to have access to such data. This category of data can also have regulatory requirements to have the keys in the same geographical region as the data. The keys might also need to be under the organization's strict custody. This content has the highest classification in your organization ("Top Secret") and access is restricted to just a few people. Highly sensitive data is what malicious users are after. Loss of this data can damage the organization's reputation and break trust with their customers.

As mentioned, Double Key Encryption is intended for your most sensitive data that is subject to the strictest protection requirements. You should do due diligence in identifying the right data to cover with this solution before you deploy. In some cases, you might need to narrow your scope and use other solutions. For example, for most of

Źródło:
https://learn.microsoft.com/en-us/purview/double-key-encryption

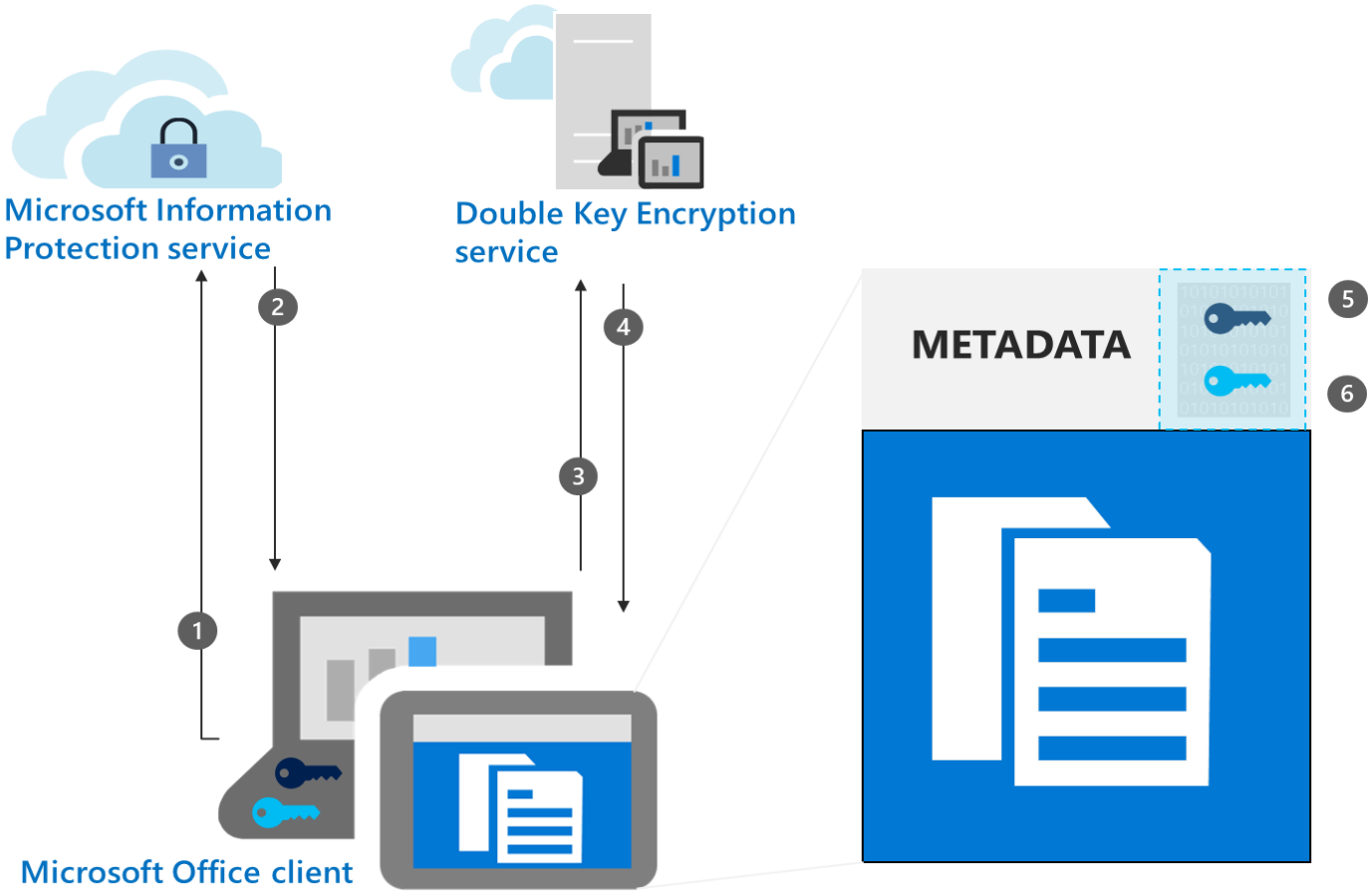
THALES

…i jeszcze jedno. To działa.

requirements. Also, these solutions enable you to use the most powerful Microsoft 365 services; services that you can't use with DKE encrypted content. For example:

- Mail flow rules including anti-malware and spam that require visibility into the attachment
- Microsoft Delve
- eDiscovery
- Content search and indexing
- Office Web Apps including coauthoring functionality
- Copilot

Jak działa podwójne szyfrowanie (DKE) w M365



Krok 1: *Bootstrapping* (uwierzytelnienie, pobranie certyfikatu użytkownika,…)

Krok 2: Pobranie i buforowanie klucza publicznego Azure Rights Management

Krok 3: Żądanie klucza publicznego DKE

Krok 4: Pobieranie i buforowanie klucza DKE

Krok 5: Ochrona dokumentu za pomocą klucza DKE

Krok 6: Ochrona dokumentu za pomocą klucza Azure

Podsumujmy do czego jest DKE

Chroni dane dwoma kluczami. Aby uzyskać dostęp do zawartości, musisz posiadać oba klucze: klucz kontrolowany przez klienta i klucz klienta w Microsoft Azure

Brak dostępu dostawcy. Ponieważ jeden klucz jest zawsze pod Twoją kontrolą, Microsoft nigdy nie ma dostępu do Twoich danych

Spójne środowisko użytkownika. Ujednolicone środowisko etykietowania w całym repozytorium danych, zarówno dla administratorów i użytkowników

THALES

Rozwiązanie:

Wsparcie DKE z Thales

DKE Service z Thales, czy może wdrożyć go samodzielnie?

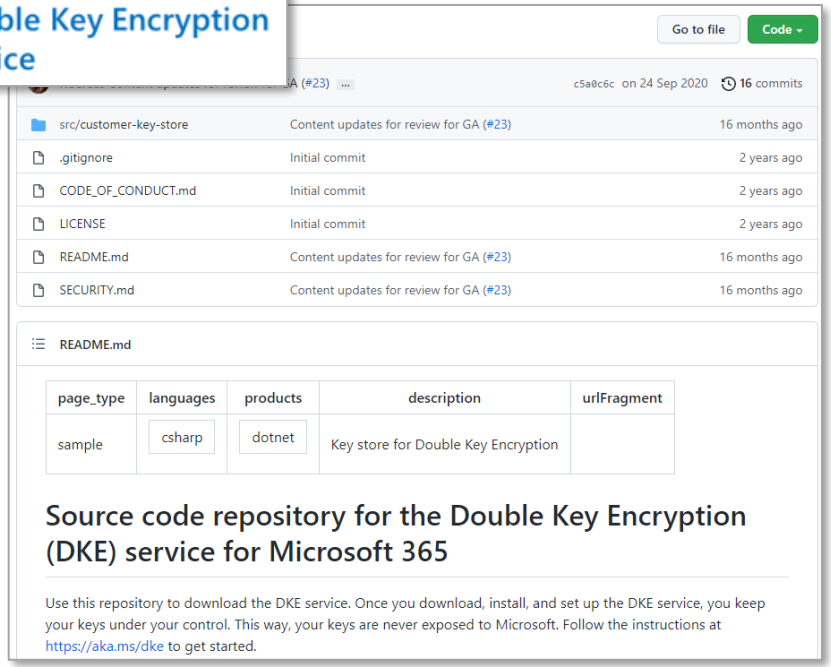
Można wdrożyć usługę Key Broker samodzielnie

Microsoft udostępnia działający przykład

- **GitHub:** https://github.com/Azure-Samples/DoubleKeyEncryptionService
- **Wideo poradnik**: https://www.youtube.com/watch?v=vDWfHN_kygg

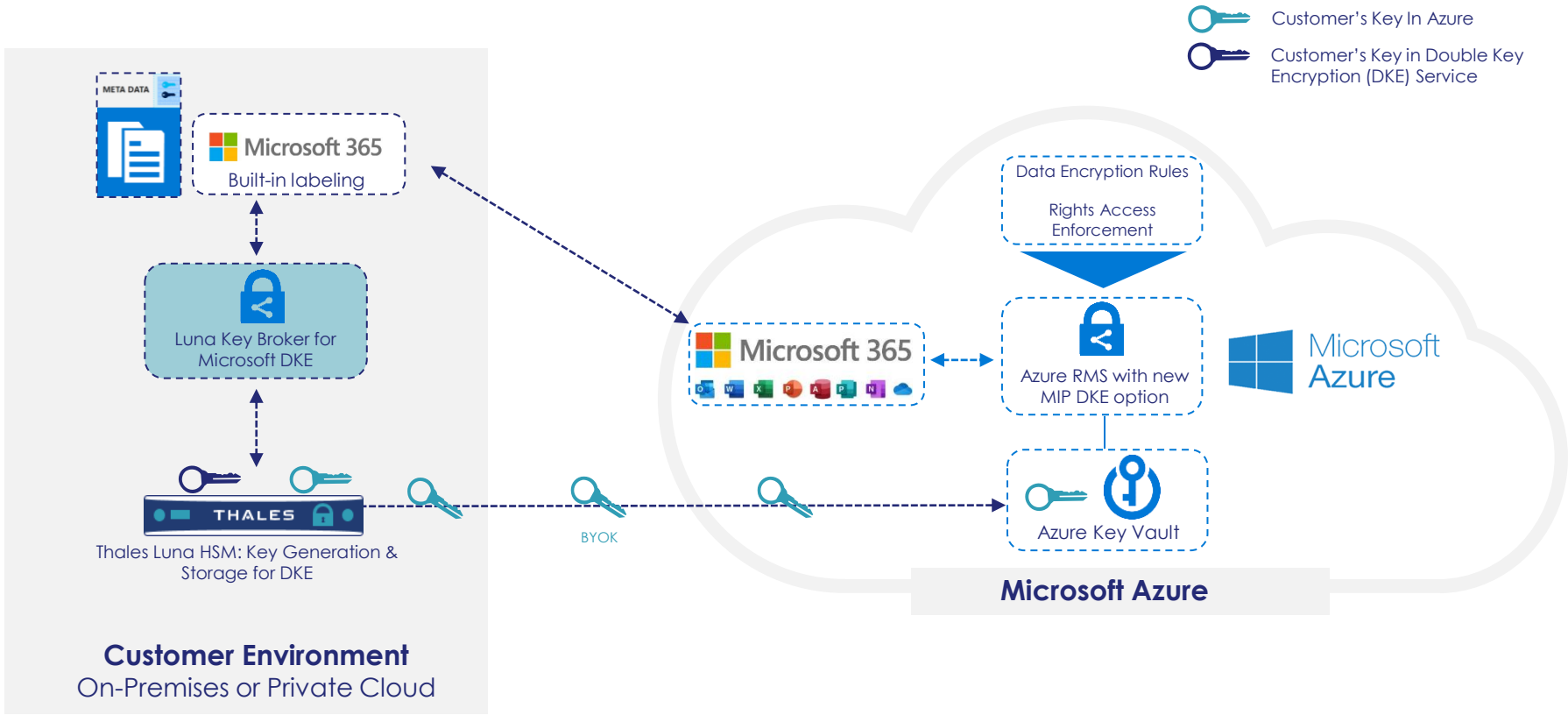
No, niby wszystko jest, ale…

- Jak przechowywane i zabezpieczone są klucze do ochrony twoich wrażliwych danych?
- Jak realizowana jest wysoka dostępność, skalowanie, backup/odtwarzanie?
- Kto będzie odpowiadał za utrzymanie i wsparcie rozwiązania?



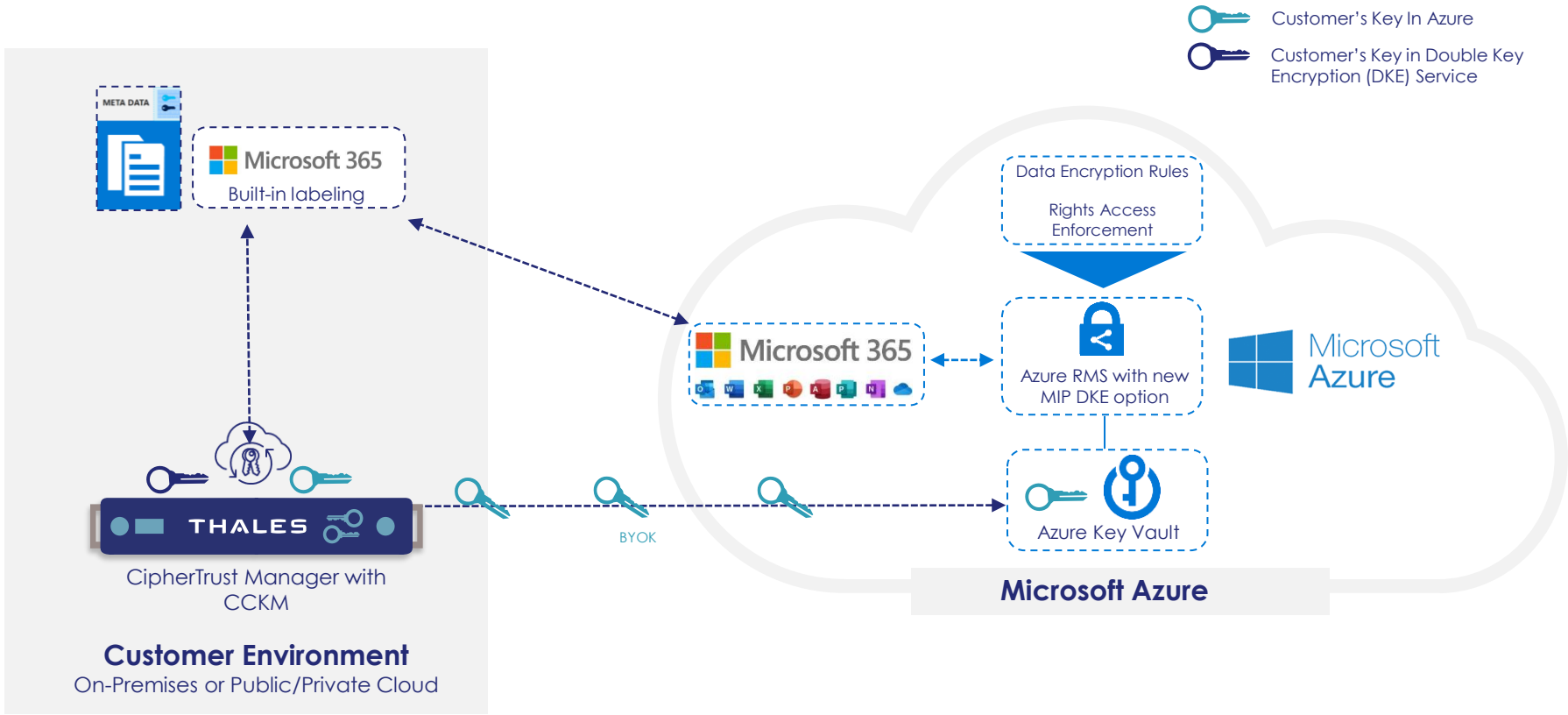
THALES

Dotychczas było: Luna Key Broker for Microsoft DKE

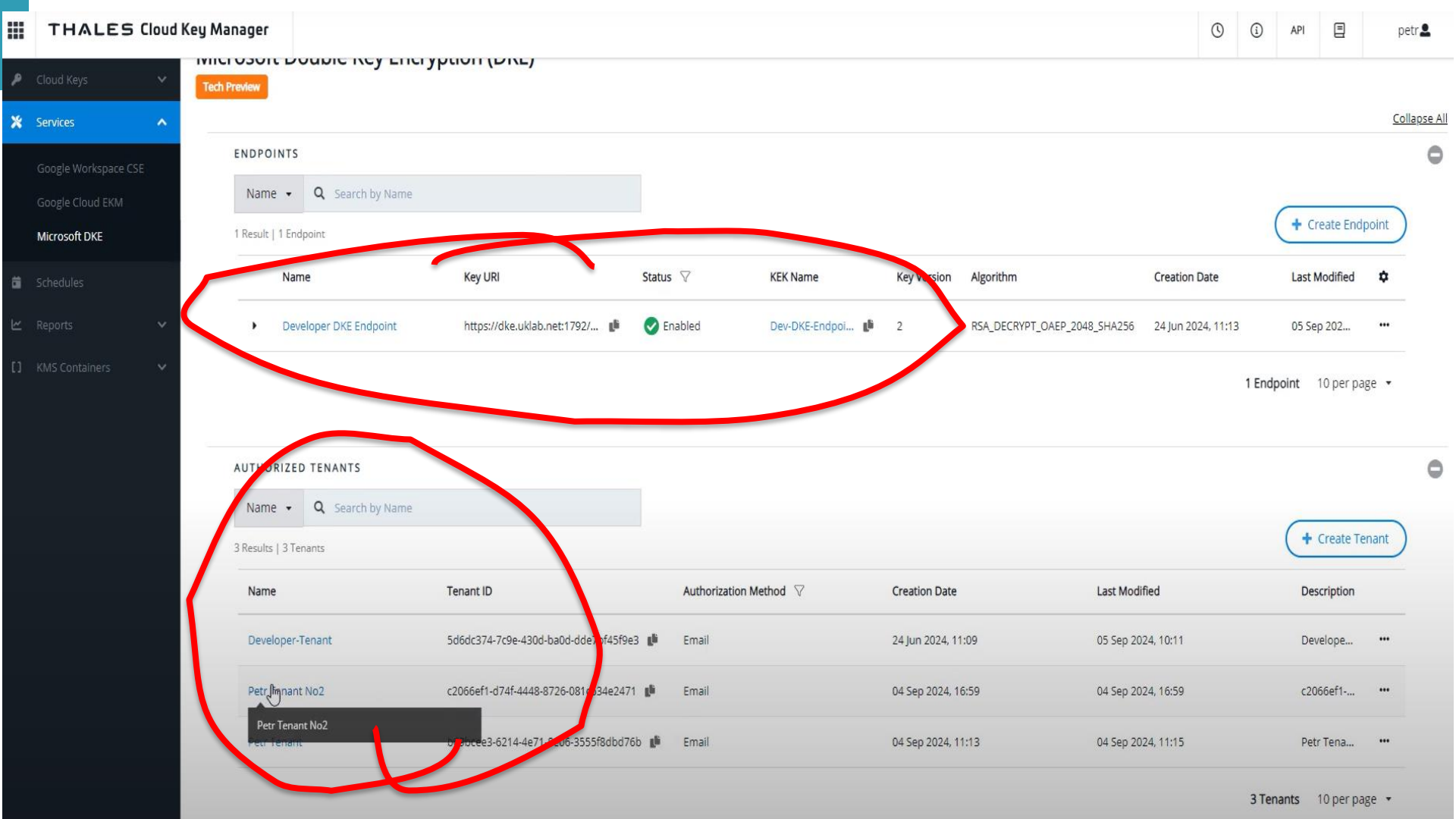


THALES

Od dziś jest także: CCKM for Microsoft DKE



THALES


THALES Cloud Key Manager
API
petr
Cloud Keys
Services
Google Workspace CSE
Google Cloud EKM
Microsoft DKE
Schedules
Reports
KMS Containers
Tech Preview
Collapse All
ENDPOINTS
Name
Search by Name
1 Result | 1 Endpoint
+ Create Endpoint
Name
Key URI
Status
KEK Name
Key Version
Algorithm
Creation Date
Last Modified
Developer DKE Endpoint
https://dke.uklab.net:1792/...
Enabled
Dev-DKE-Endpoi...
2
RSA_DECRYPT_OAEP_2048_SHA256
24 Jun 2024, 11:13
05 Sep 202...
1 Endpoint
10 per page
AUTHORIZED TENANTS
Name
Search by Name
3 Results | 3 Tenants
+ Create Tenant
Name
Tenant ID
Authorization Method
Creation Date
Last Modified
Description
Developer-Tenant
5d6dc374-7c9e-430d-ba0d-dde
f45f9e3
Email
24 Jun 2024, 11:09
05 Sep 2024, 10:11
Develope...
Petr Tenant No2
c2066ef1-d74f-4448-8726-081
34e2471
Email
04 Sep 2024, 16:59
04 Sep 2024, 16:59
c2066ef1-...
Petr Tenant No2
Email
04 Sep 2024, 11:13
04 Sep 2024, 11:15
Petr Tena...
3 Tenants
10 per page

Edit sensitivity label

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

User access to content expires

Never

Allow offline access

Always

Assign permissions to specific users and groups *

Assign permissions

7 items

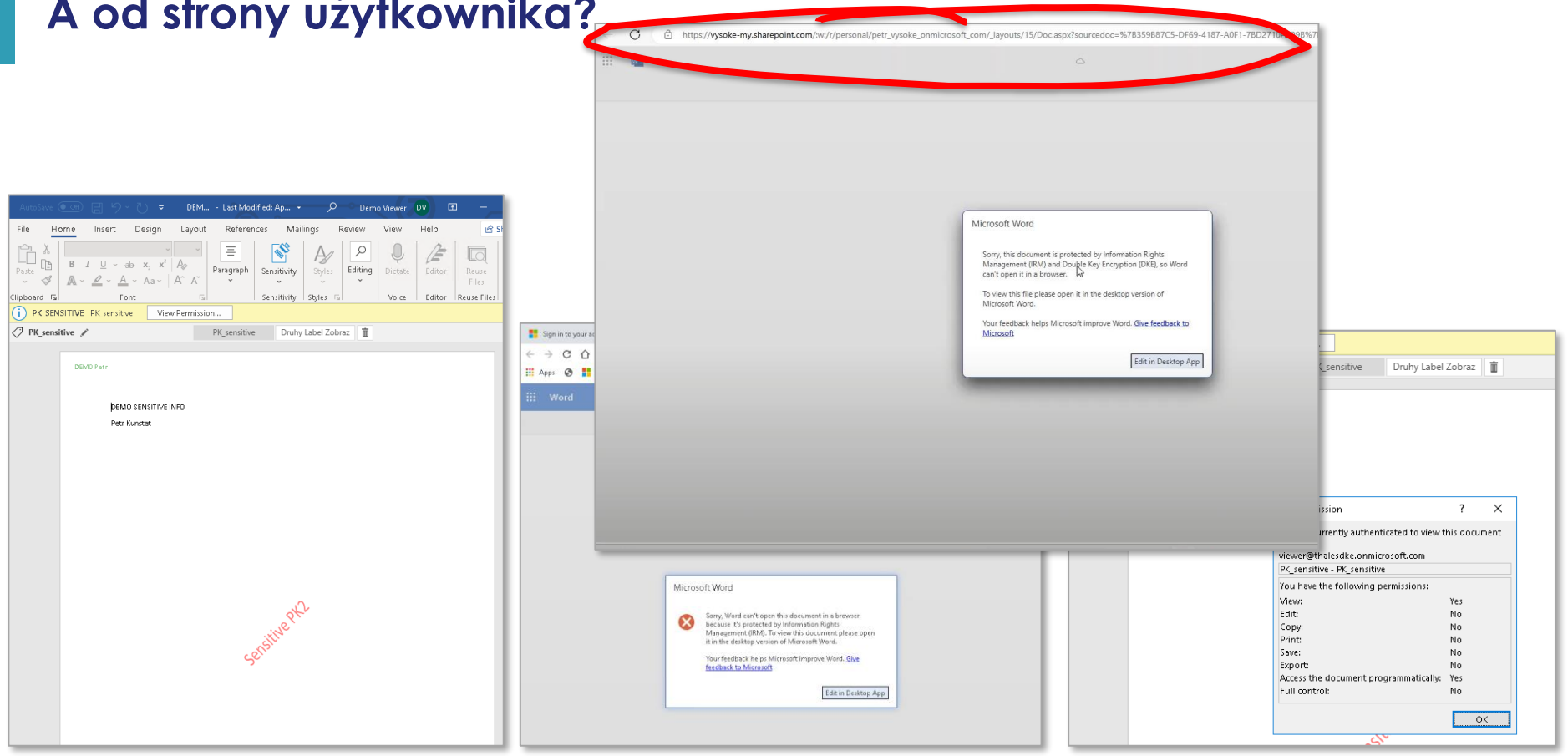
Users and groups	Permissions	Edit	Delete
ThalesCEE5@vysoke.onmicrosoft.com	Co-Author		
allcompany@vysoke.onmicrosoft.com	Co-Author		
demo@vysoke.onmicrosoft.com	Co-Author		
petr@vysoke.onmicrosoft.com	Co-Author		
reader@vysoke.onmicrosoft.com	Co-Author		
vysoke.onmicrosoft.com	Co-Author		
writer@vysoke.onmicrosoft.com	Co-Author		

Use dynamic watermarking

Use Double Key Encryption

https://dke.uklab.net:1792/api/v1/cckm/microsoft/dke-data-plane/endpoints/2838fdad-c90c-4f91-88a3-29436b7fd682/keys/Dev-DKE-Endpoint-Key

A od strony użytkownika?



O czym warto pamiętać lub nie znajdziecie w dokumentacji #1/1

Do jakich URLi odwołuje się aplikacja Office kontaktując się z *DKE Service*?

- Są to:
  - https://<host>/<pubkey>
  - https://<host>/<pubkey>/<ID>/decrypt

Czy każdy użytkownik Office/Microsoft 365 może korzystać z DKE?

- *Double Key Encryption for Microsoft 365 comes with Office 365* ***E5*** *or Microsoft 365* ***E5****.*

Czym różni się DKE od HYOK?

- *Double Key Encryption encrypts your data* ***with two keys.*** *Your encryption key is* ***in your control*** *and the second key is stored in Microsoft Azure, allowing you to move your encrypted data to the cloud.* ***HYOK*** *protects your content* ***with only one key*** *and the* ***key is always on premises****.*

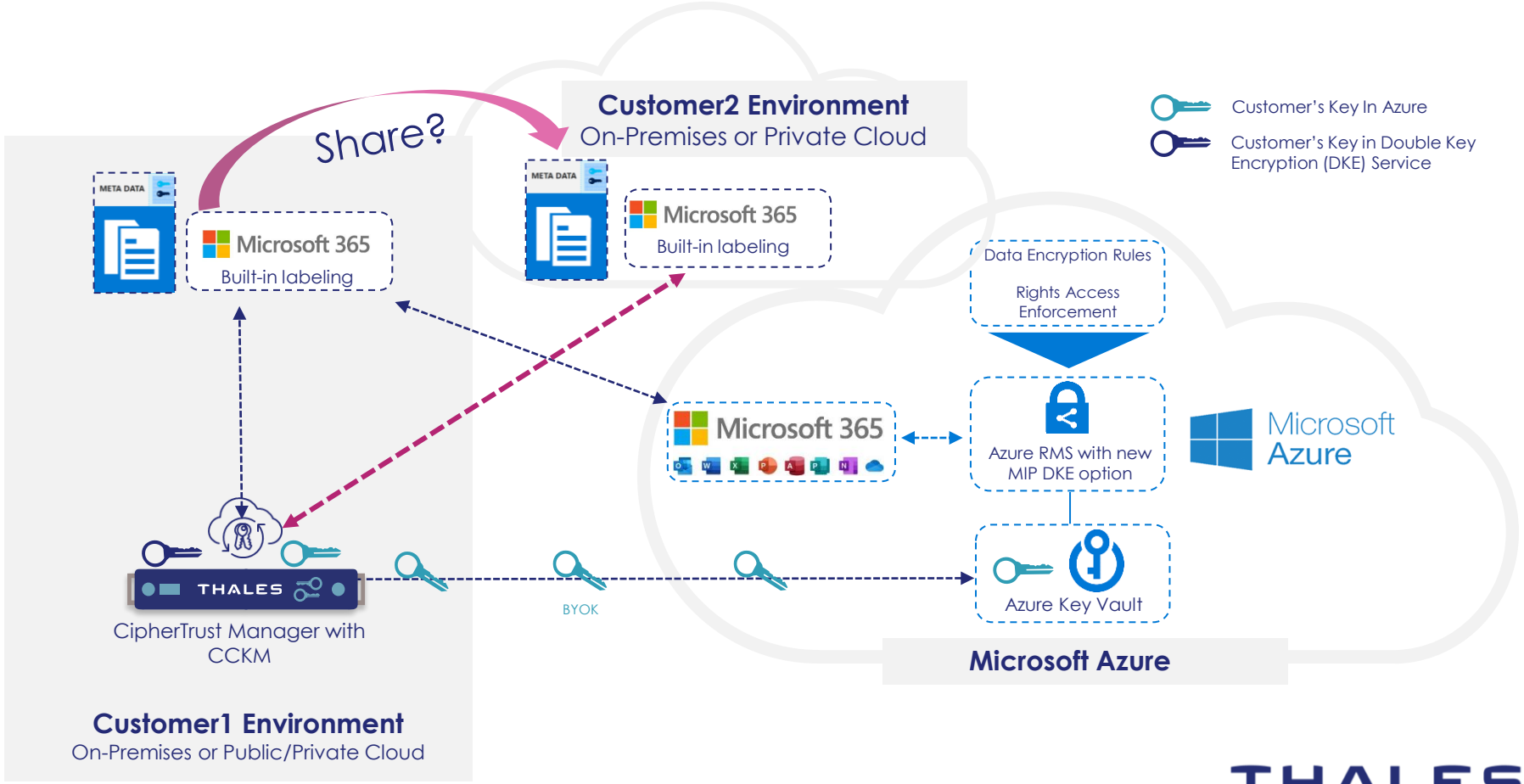
Microsoft DKE consumes one CCKM license (cloud unit) per endpoint. One CCKM DKE endpoint can be used to create one or more labels across one or more Azure tenants.

Aktywacja DKE w CCKM?

Czy dokumenty zabezpieczone DKE mogą być udostępniane zewnętrznie?

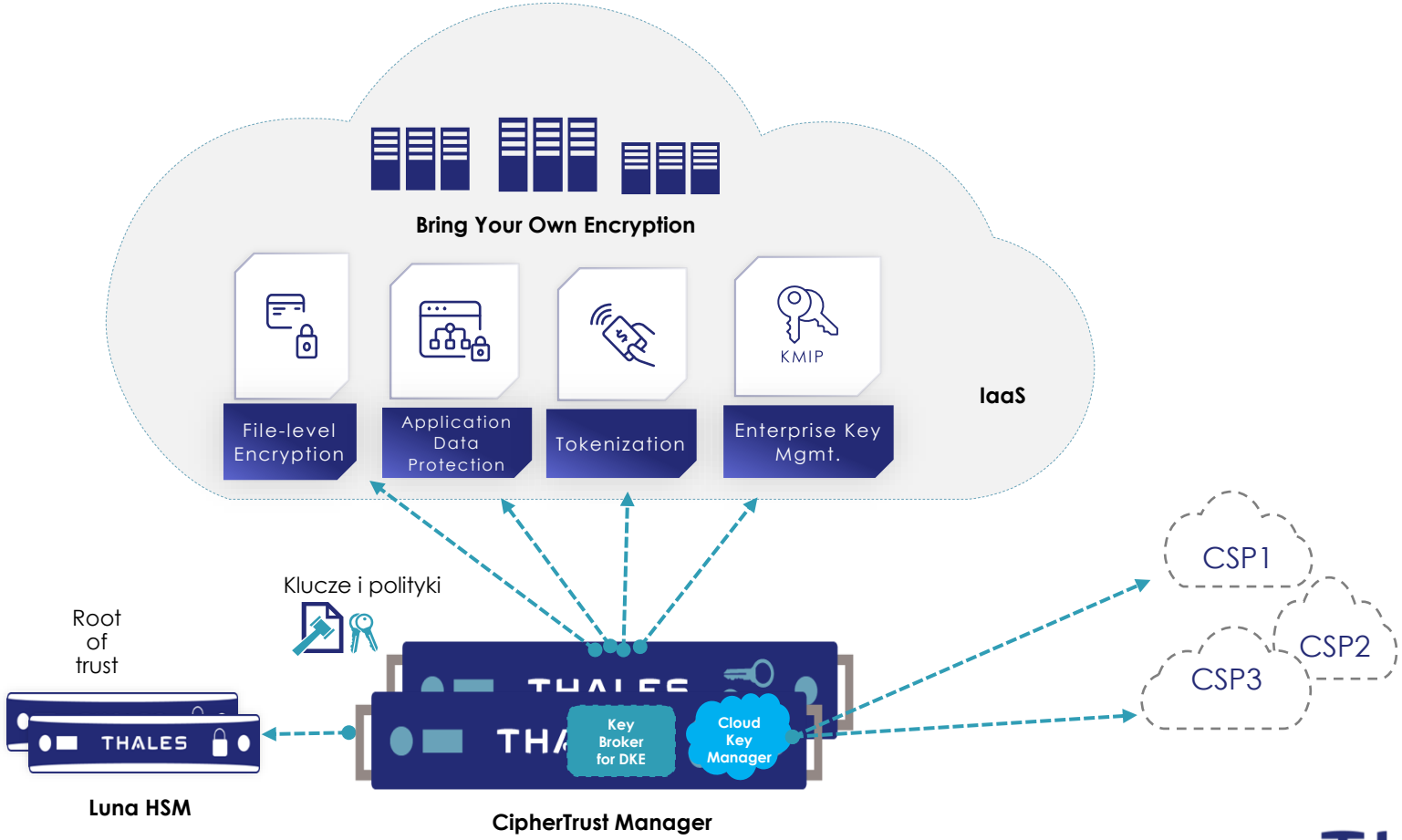
- Tak! Pod kilkoma warunkami…

Udostępnianie dokumentów zabezpieczonych DKE w grupie firm?



THALES

Czy można chronić zasoby Azure za pomocą DEK? Nie, ale…

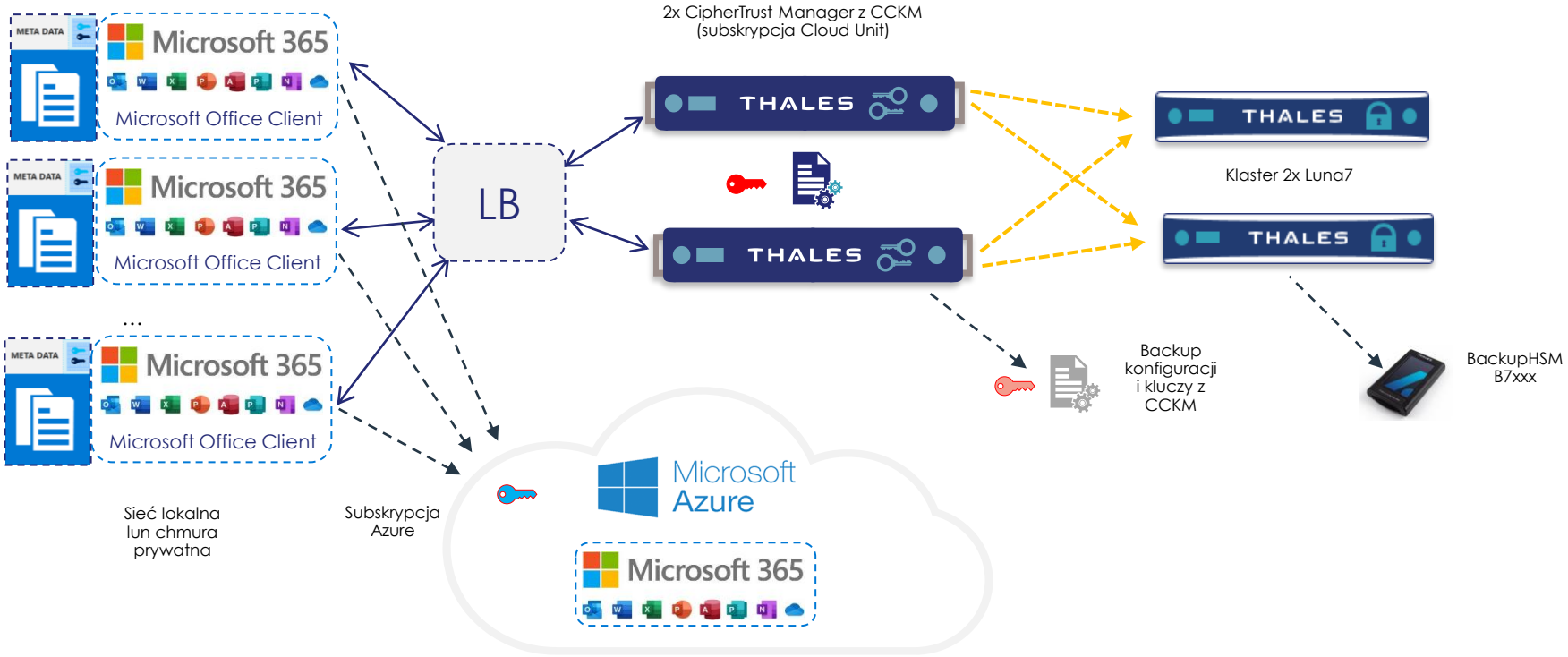


THALES

CryptoPanel

podsumowanie

Problem i propozycja rozwiązania



Czego potrzebujemy aby zaoferować DKE w integracji z CCKM:

- **DKE łatwo wdrożyć z użyciem CCKM**
- **Dla wymagających:**
  - Możliwość wdrożenia klastra HA/LB oraz
  - Kopia kluczy DKE na wypadek DR

- **produkty dostępne w kanale partnerskim**
- **licencja dożywotnia lub subskrypcja**
- **licencja ewaluacyjna do testów (na 90dni)**

BOM:

- **2x CipherTrust Manager - 2x 7k €**
- **1x Cloud Unit – 13k €**
- **Opcjonalnie:**
  - 2x Luna A700 – 2x 18k €
  - 1x Luna Backup HSM B700 – 1x 6k €
  - ~~0x Luna Client License!~~

Podsumowanie

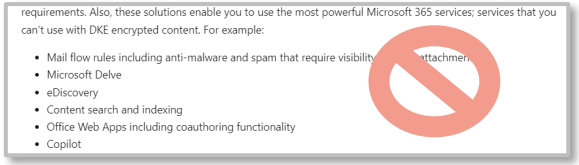
DKE to rozwiązanie wprowadzone w M365 dla zapewnienia poufność szczególnie wrażliwych danych (dokumentów)

- Chroni dane w spoczynku, przesyle i użyciu

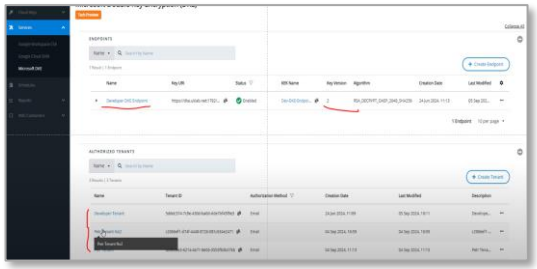
Dzięki wdrożeniu *DKE Service* we własnych zasobach, dane nigdy nie są w postaci jawnej dostępne na platformie Azure,

Thales CCKM pozwala łatwo ustanowić *DKE Service* i chronić klucze

- Wdrożenie klaster wysokiej dostępności
- Wiele kluczy dla różnych grup użytkowników (tenantów)
- Wiele etykiet wrażliwości, każda z własnym kluczem
- Rotowanie kluczy (rollover)
- Backup/odtwarzanie materiału
- Zawiadywanie kluczami (BYOK) w Azure KeyVault z tej samej konsoli
- …


requirements. Also, these solutions enable you to use the most powerful Microsoft 365 services; services that you can't use with DKE encrypted content. For example:

- Mail flow rules including anti-malware and spam that require visibility [illegible] attachment
- Microsoft Delve
- eDiscovery
- Content search and indexing
- Office Web Apps including coauthoring functionality
- Copilot



CryptoPanel

CryptoPanel

A teraz quiz z upominkami