

CryptoPanel

edycja #3

Zabezpieczanie danych wrażliwych w magazynach chmurowych Azure Storage. BYOK albo HYOE.



CryptoPanel

dziś dyskutują



Joanna Rzepka

Channel Sales Manager

joanna.rzepka@thalesgroup.com

mob. +48 600 537 666



Jarosław Ulczok

Pre-sales Consultant

Jaroslaw.Ulczok@thalesgroup.com

mob. +48 603 056 667



CryptoPanel



problem

co nas boli...

- Jesteśmy firmą, która przetwarza znaczne ilości wrażliwych danych.
- Posiadane zasoby magazynów danych wystarczają do codziennej obsługi ale nie są wystarczające do długoterminowego składowania takich ilości danych do czego jesteśmy zobligowani.
- Poszukujemy taniego rozwiązania do bezpiecznego przechowywania danych na długie okresy czasu (miesiące, lata).
- Znamy i wykorzystujemy Azure Storage oraz funkcjonalność BYOK. Nie do końca spełnia ono nasze wymagania (KNF).
- Podlegamy regulacji w zakresie ochrony danych osobowych (RODO traktujemy poważnie) i rynku regulowanego przez KNF.
- ...koszt powiększania i utrzymania zasobów magazynów danych ciąży w rozliczaniach działu IT.
- ...jak zapewnić bezpieczeństwo danych gdy są one składowane poza firmą (np. w chmurze)? Jak zautomatyzować taki proces?
- ...jak usprawnić zarządzanie kluczami w wykorzystywanych usługach w ramach Azure?
- ...musimy posiadać możliwość odtworzenia wrażliwych danych z zasobów archiwalnych. Czas dostępu do tych danych nie jest krytyczny (dni).
- ...jak wykazać, że dane są właściwie chronione (zwłaszcza przed audytorem)?



Czym właściwe jest Azure Storage?

Znajdź odpowiedni dla siebie produkt z zakresu magazynu

JEŚLI CHCESZ	UŻYJ TEGO
Magazyn blokowy o wysokiej wydajności i trwałości dla usługi Azure Virtual Machines	Azure Disk Storage
Wysoce skalowalny i bezpieczny magazyn obiektów przeznaczony do natywnych dla chmury obciążeń, archiwów, repozytoriów typu data lake, obliczeń o wysokiej wydajności i uczenia maszynowego	Azure Blob Storage
Wysoce skalowalny i bezpieczny magazyn typu data lake dla obciążeń analizy o wysokiej wydajności	Azure Data Lake Storage
Proste, bezpieczne i bezserwerowe udziały plików w chmurze klasy korporacyjnej	Usługa Pliki systemu Azure
Magazyn plików przedsiębiorstwa, obsługiwany przez usługę NetApp	Azure NetApp Files
Urządzenia i rozwiązania do transferu danych w trybie offline na platformę Azure	Urządzenie Azure Data Box
Store unstructured data that is completely tamper-proof and can be cryptographically verified	Microsoft Azure Confidential Ledger

Źródło: <https://azure.microsoft.com/pl-pl/product-categories/storage/>

Środowiska cloudowe vs. praktyki i rozporządzenia

Komunikat UKNF Chmura Obliczeniowa 68669

4. Nadzór uznaje ochronę przetwarzania informacji istotnych dla procesów lub działalności podmiotu nadzorowanego lub stanowiących informacje prawnie chronione za zagrożenie o charakterze priorytetowym. Stosowanie nieodpowiednich reżimów prawnych w tym zakresie może wywołać negatywne konsekwencje dla funkcjonowania rynku finansowego oraz wpływa na możliwość wykonywania efektywnego nadzoru nad procesami przetwarzania informacji. Obowiązujące na terenie Europejskiego Obszaru

23) **ujawnienie informacji** – bez uszczerbku dla rozumienia przepisów prawa bezwzględnie obowiązujących, oznacza sytuację, podczas której informacje są przetwarzane w chmurze obliczeniowej:

- w sposób nieszyfrowany albo
- w sposób zaszyfrowany „at rest” lub „in transit”, ale dostęp do kluczy szyfrujących i szyfrowanej tymi kluczami informacji posiada albo może posiadać dostawca usług chmury obliczeniowej lub jego poddostawca w łańcuchu outsourcingowym.

5) stanowisko nadzoru w sprawie szyfrowania informacji, zgodnie z którym:

- szyfrowanie informacji nie zmniejsza ważności informacji, nie zmienia też jej klasyfikacji i oceny;
- szyfrowanie informacji oraz właściwe zarządzanie kluczami szyfrującymi zapobiega ujawnieniu informacji;
- brak jest gwarancji dla uznania danego algorytmu szyfrowania za całkowicie bezpieczny” Nadzór zaleca używanie algorytmów

CryptoPanel



rozwiązanie



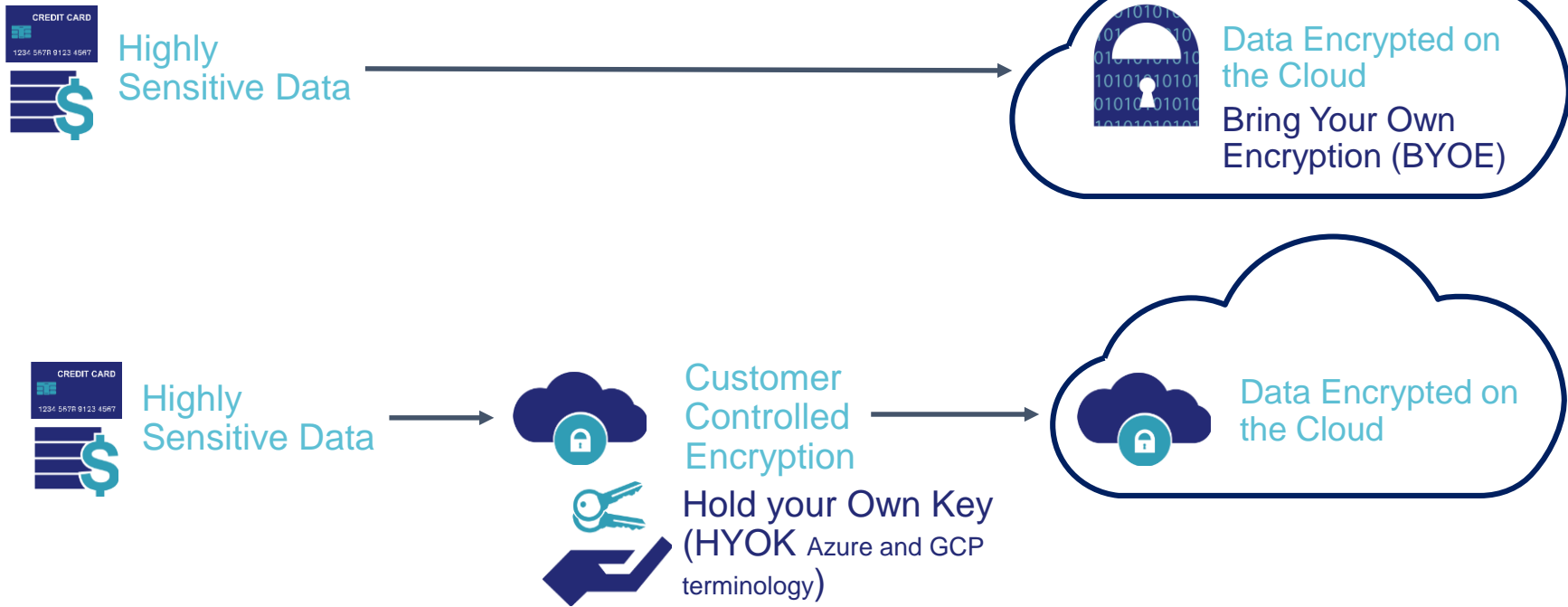
Rozwiązania dwa:

1. CM (z CCKM Embedded) w integracji z Azure (Storage) - **BYOK**

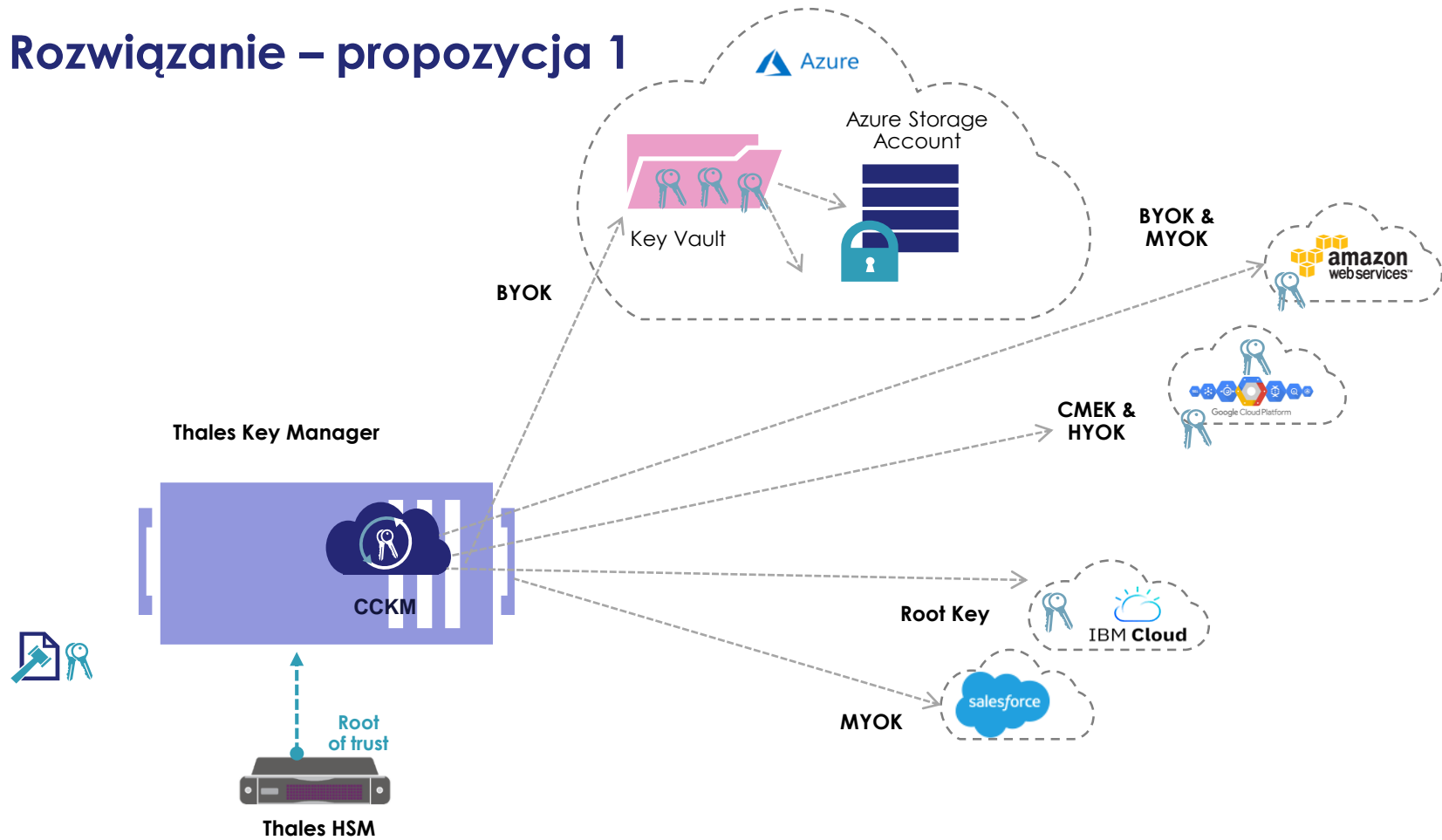
2. Szyfrowanie zasobów z wykorzystaniem CTE przed składowaniem w Azure Storage - **HYOE**



HYOE – Klient dostarcza szyfrowanie i klucze



Rozwiązanie – propozycja 1



Tworzenie magazynu danych i jego szyfrowanie

Blob storage

Enable network file share v3

Azure Files

Enable large file shares

Tables and Queues

Enable support for customer-managed keys

Access tier

Hot: Frequently accessed data and day-to-day usage scenarios

Cool: Infrequently accessed data and backup scenarios

Security + networking

This option cannot be changed after this sto

Home > ccejstorage

ccejstorage | Encryption

Storage account

Search (Ctrl+/)

Encryption Encryption scopes

Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in our datacenters, and automatically decrypts it for you as you access it.

Please note that after enabling Storage Service Encryption, only new data will be encrypted, and any existing files in this storage account will retroactively get encrypted by a background encryption process. [Learn more about Azure Storage encryption](#)

Infrastructure encryption Disabled

Encryption type

Microsoft-managed keys

Customer-managed keys

Key selection

Current key

Automated key rotation

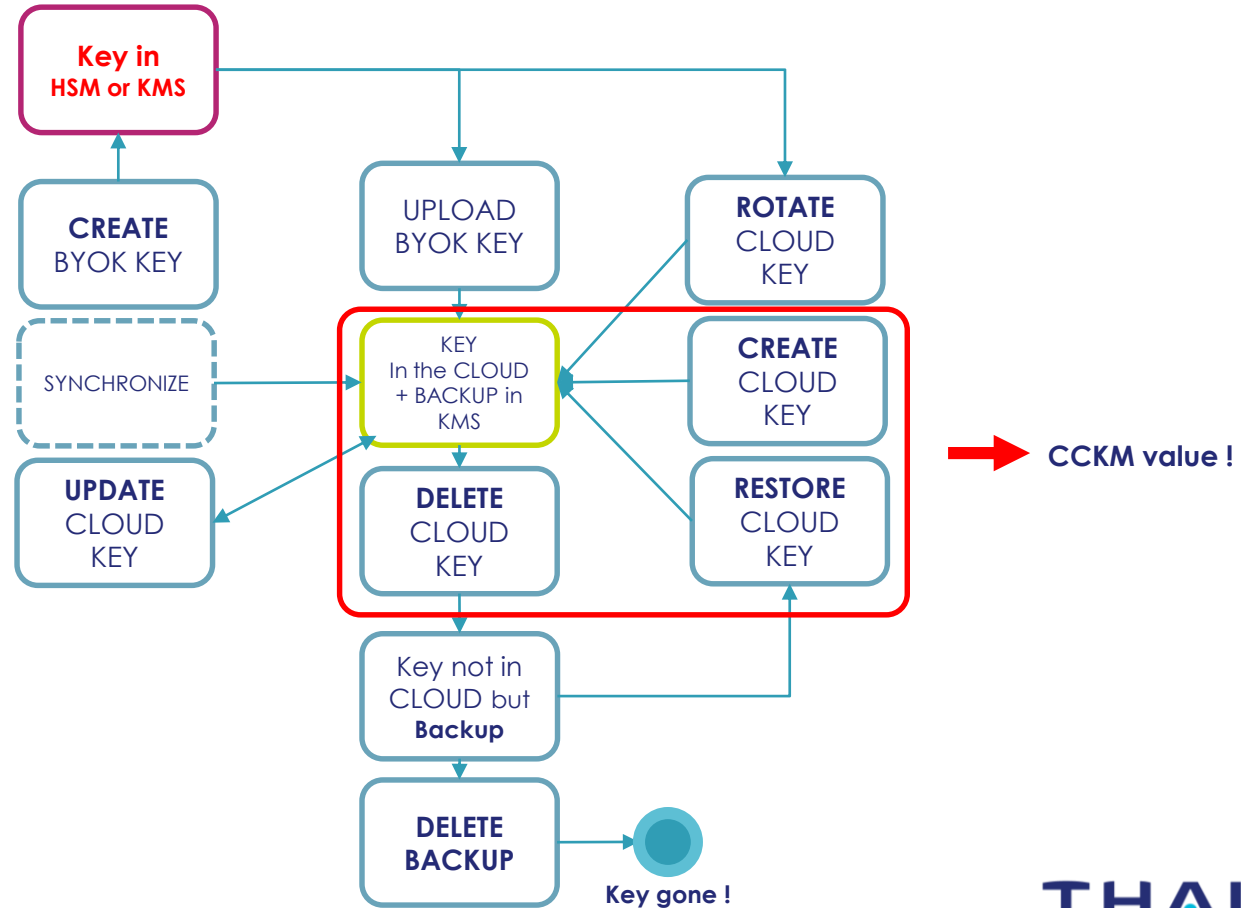
Key version in use

[Change key](#)

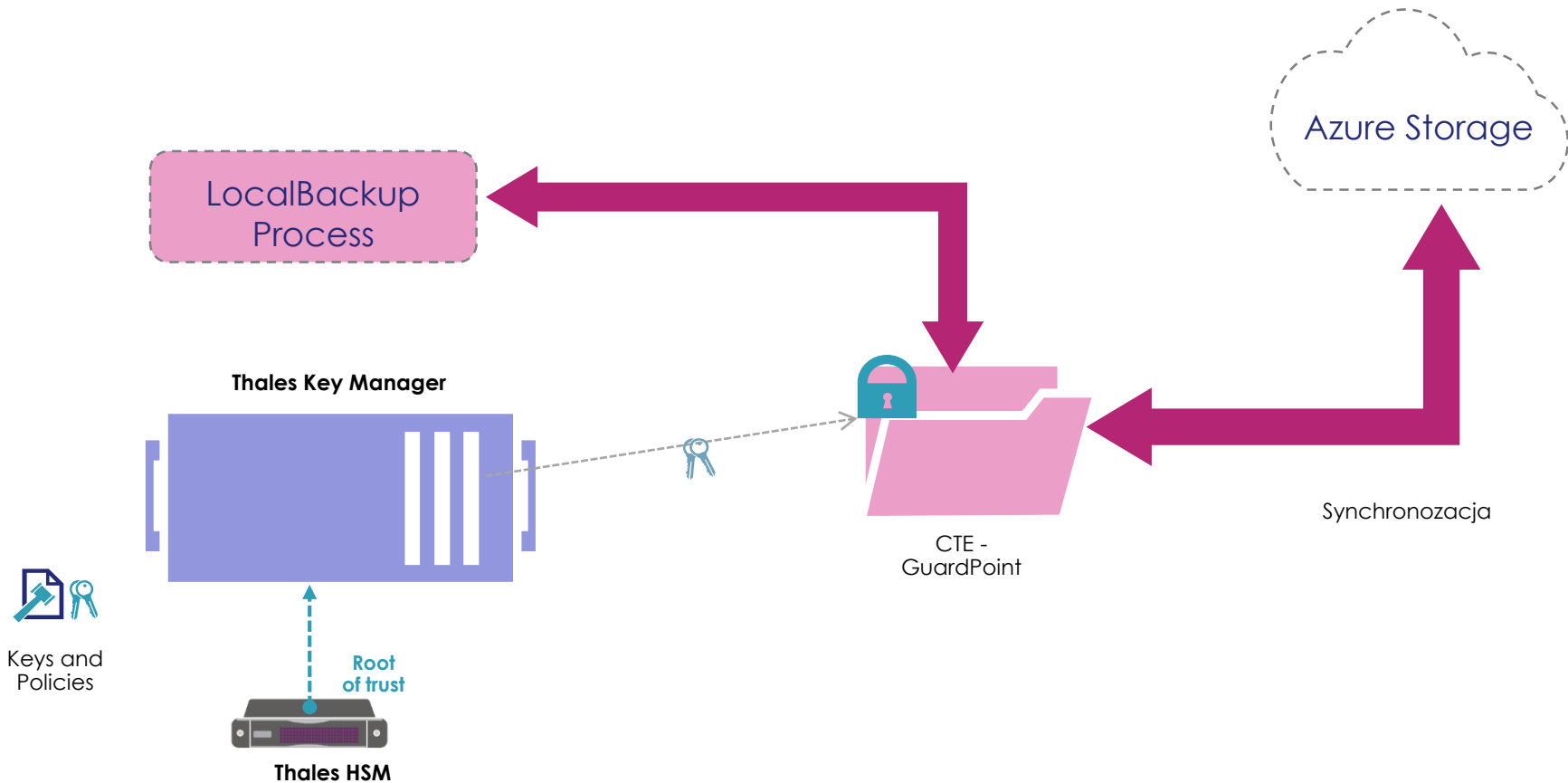
How likely to a fri

Not at

CCKM co w zasadzie daje? Disaster Recovery by design !



Rozwiązanie – propozycja 2 (HYOE)



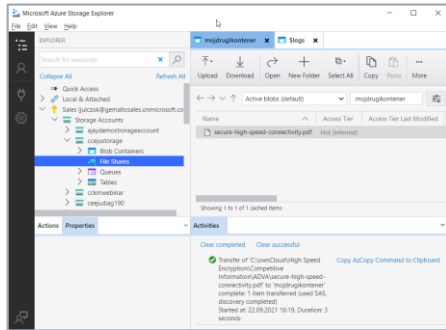
Rozwiązanie – propozycja 2

#	Resource	User	Process	Action	Effects
1	..\<share>/*.*	Authorized	LocalbackupProcess	Write/Read	Permit, Encrypt/Decrypt
2	..\<share>/*.*	Authorized	AZCOPY	Read	Permit, Audit
2	..\<share>/*.*	Authorized	AZCOPY	Write	Permit, ????
2	..\<share>/*.*	Administrators	Whitelisted management process	Metadata Only	Permit, Audit
3	..\<share>/*.*	*	*	*	Deny, Audit



AZCOPY sync 'C:\myShare' 'https://JUStorage.blob.core.windows.net/mycontainer' --recursive

AZCOPY sync 'https://JUStorage.blob.core.windows.net/mycontainer' 'C:\myShare' --recursive



\myShare



„Nauczki“, czyli lessons learned #1/2

❖ Dlaczego nie mogę dodać (nie widzę) mojego KeyVault w CM pomimo poprawne podłączenia subskrypcji Azure ?

❖ Odpowiedź: CCKM pracuje w Azure w ramach przypisanego konta aplikacji. Należy mu nadać odpowiednie uprawnienia w ramach kontroli dostępu do Vaulta

Add Existing Key Vaults

Select a connection from CipherTrust Connection Management. The selected connection will be used to connect to the vaults, and the subscription selected will provide a list of associated key vaults.

Azure Connection
JU Azure

Subscription
Sales (7a79a515-9e31-43ac-a1c5-a1714d4d2455)

Search by Vault Name

0 Selected 3 Results | 3 Vaults

Vault Name	Vault URI
<input type="checkbox"/> CCKM-demo-JU	https://cckm-demo-ju.vault.azure.net/
<input type="checkbox"/> CCKM-demo-JUStorage	https://cckm-demo-ju-storage.vault.azure.net/
<input type="checkbox"/> JUVault4Storage	https://juvault4storage.vault.azure.net/

Key vaults - Microsoft Azure

Home > Key vaults

Filter for any field... Subscription == all Resource group == all

Showing 1 to 4 of 4 records.

Name	Type
<input type="checkbox"/> CCKM-demo-JU	Key vault
<input type="checkbox"/> CCKM-demo-JUStorage	Key vault
<input type="checkbox"/> CCKMClcoPM	Key vault
<input type="checkbox"/> JUVault4Storage	Key vault

Key vaults CCKM-demo-JU

Assignments for the selected user, group, service principal, or managed identity at this scope

Search (Ctrl+/) Search by assignment name or description

Filter for any field...

Role assignments (2)

Role	Description	Scope
Key Vault Contributor	Lets you manage key vaults, but n...	This resource
Owner	Grants full access to manage all re...	Subscription (Inherited)

Deny assignments (0)

Classic administrators (0)

Key vaults CCKMClcoPM

Assignments for the selected user, group, service principal, or managed identity at this scope

Search (Ctrl+/) Search by assignment name or description

Filter for any field...

Role assignments (1)

Role	Description	Scope
Owner	Grants full access to manage all re...	Subscription (Inherited)

Deny assignments (0)

Classic administrators (0)



„Nauczki“, czyli lessons learned #1/2

Azure Storage ma podwójne szyfrowanie ale... [czy można kontrolować klucze?]

- Włączanie szyfrowania infrastruktury w celu podwójnego szyfrowania danych: <https://docs.microsoft.com/pl-pl/azure/storage/common/infrastructure-encryption-enable?tabs=portal>

Konto magazynu danych może automatycznie rotować klucz szyfrujący w chwili tak rotacji kucza w CCKM

The screenshot displays the Azure Key Vault management console. On the left, the 'myFISTkey' page shows a table of key versions. A red arrow points from the first version ID, 'c321824d8c3...', to the 'Key version in use' field in the 'Encryption selection' dialog box.

Version ID	Type
c321824d8c3...	RSA
0922e9c2e8b...	RSA
0dcba80e95f...	RSA

Encryption selection

Enable support for customer-managed keys

All service types (blobs, files, tables, and queues)

Infrastructure encryption Disabled

Encryption type

Microsoft-managed keys

Customer-managed keys

Key selection

Current key `https://cckm-demo-justorage.vault.azure.net/keys/myFISTkey`

Automated key rotation **Enabled - Using the latest key version**

Key version in use `c321824d8c344ff087caf06ad3c13f12`

[Change key](#)

Tego raczej nie znajdziecie w dokumentacji....

...Our customer is looking for some information about how CCKM embedded talks to Cloud KMS (AWS , Azure). They wanted to know if we have details of the workings. Does CCKM simply use the BYOK API with nothing proprietary added? I believe the answer is yes, but was looking for something in the doc that just says that in plain written word...

I don't know if that is spelled out explicitly in the docs, but yes, **we use nothing proprietary**. Just AWS, or Azure published, public API.

[CTE PM]: Considering Azure is increasing its market share we are working to prioritize a CTE feature to support encryption of Azure Blob files similar to CTE COS S3 feature.

Czyli będzie jeszcze łatwiej!

Pytania i odpowiedzi (Q&A) w zakresie stosowania Komunikatu UKNF z 23 stycznia 2020 r. dotyczącego przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej

https://www.knf.gov.pl/dla_rynku/fin_tech/chmura_obliczeniowa/Q&A



CryptoPanel



podsumowanie



Podsumowanie i słowo o tym „no to co potrzeba”?

CM (Z CCKM Embedded) szybko i łatwo integruje się z Azure (Storage) (BYOK)

- Centralne zarządzanie kluczami, „ułatwiacz” w obsłudze PAI
- Dostępna automatyczna rotacja kluczy na koncie usługi magazynu

Dla wymagających pomagamy z koncepcją HYOE: CTE + CM

produkty dostępne w kanale partnerskim

licencja dożywotnia lub subskrypcja

licencja demo do testów

zalecane użycie urządzenia HSM

Opcja 1 BYOK

CipherTrust Manager – 14,5k euro netto

CipherTrust Cloud Key Manager – 10,8K euro netto

Opcja 2 HYOE

CipherTrust Manager – 14,5k euro netto

CipherTrust Flex Connector – 4,5K euro netto



CryptoPanel



Materiały

▮ Oprogramowanie do pobrania lub wersja ewaluacyjna...

- W takim przypadku prosimy o kontakt z nami!

▮ Dokumentacja...

- CipherTrust Manger: <https://www.thesdocs.com/ctp/cm/latest/>
- CCKM Azure – integracja:
https://www.thesdocs.com/ctp/cm/latest/admin/cckm_ag/azure/index.html
- CTE: <https://www.thesdocs.com/ctp/cte/Books/Online-Files/index-7.1.1.html>

▮ Zapraszamy także na...

THALES TRUSTED ACCESS SUMMIT, 5-6 October 2021

