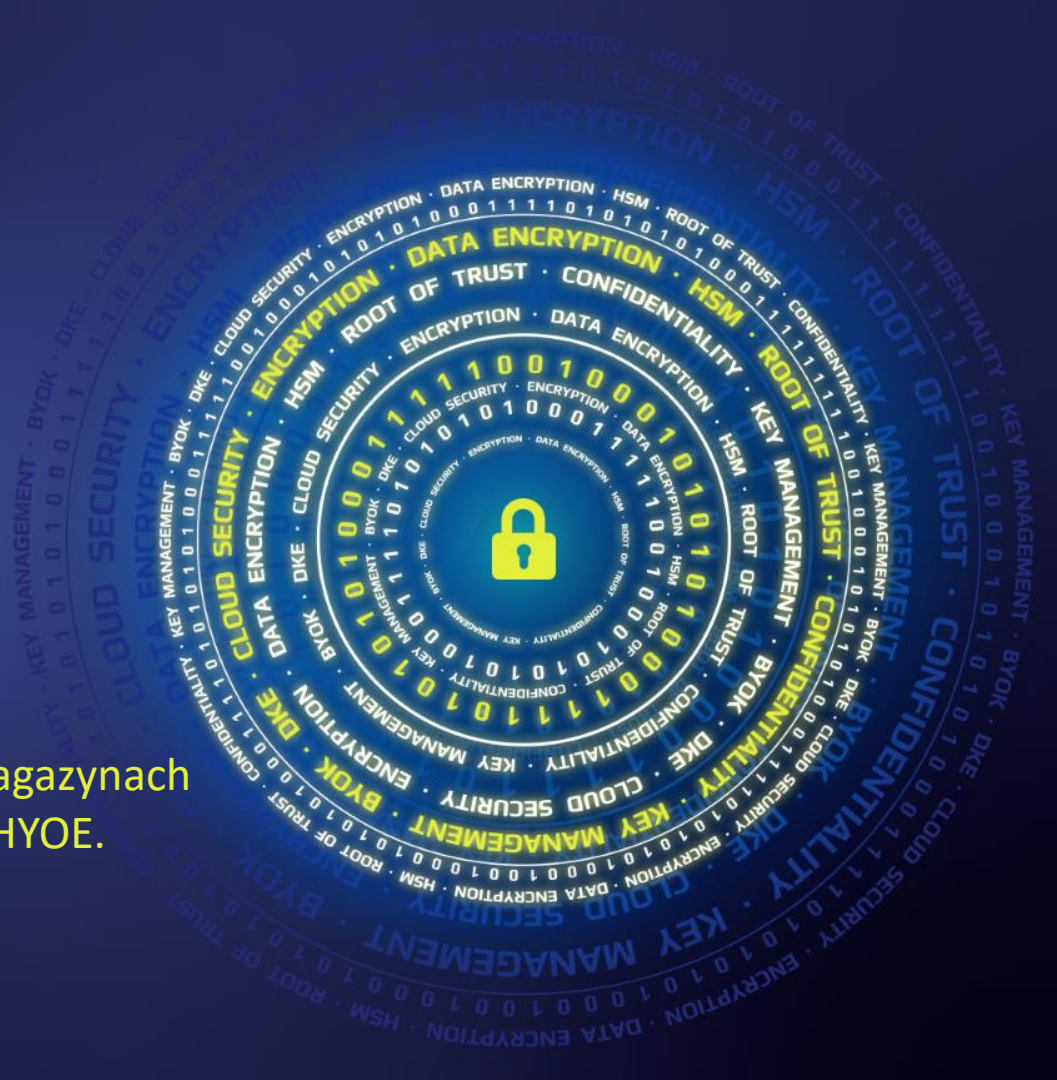
CryptoPanel

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 ciążyć w rozliczaniach działu IT.
- ...jak zapewnić bezpieczeństwo danych gdy są one składowane poza firmą (np. w chmurze)? Jak zautomatyzować taki proces?
- …jak usprawnić zarządzenie 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/

THALES

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 zagadnienie 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:
   a) w sposób nieszyfrowany albo
   b) 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:
   a) szyfrowanie informacji nie zmniejsza ważności informacji, nie zmienia też jej klasyfikacji i oceny;
   b) szyfrowanie informacji oraz właściwe zarządzanie kluczami szyfrującymi zapobiega ujawnieniu informacji;
   c) brak jest gwarancji dla uznania danego algorytmu szyfrowania za całkowicie bezpieczny". Nadzór zaleca używanie algorytmów

CryptoPanel

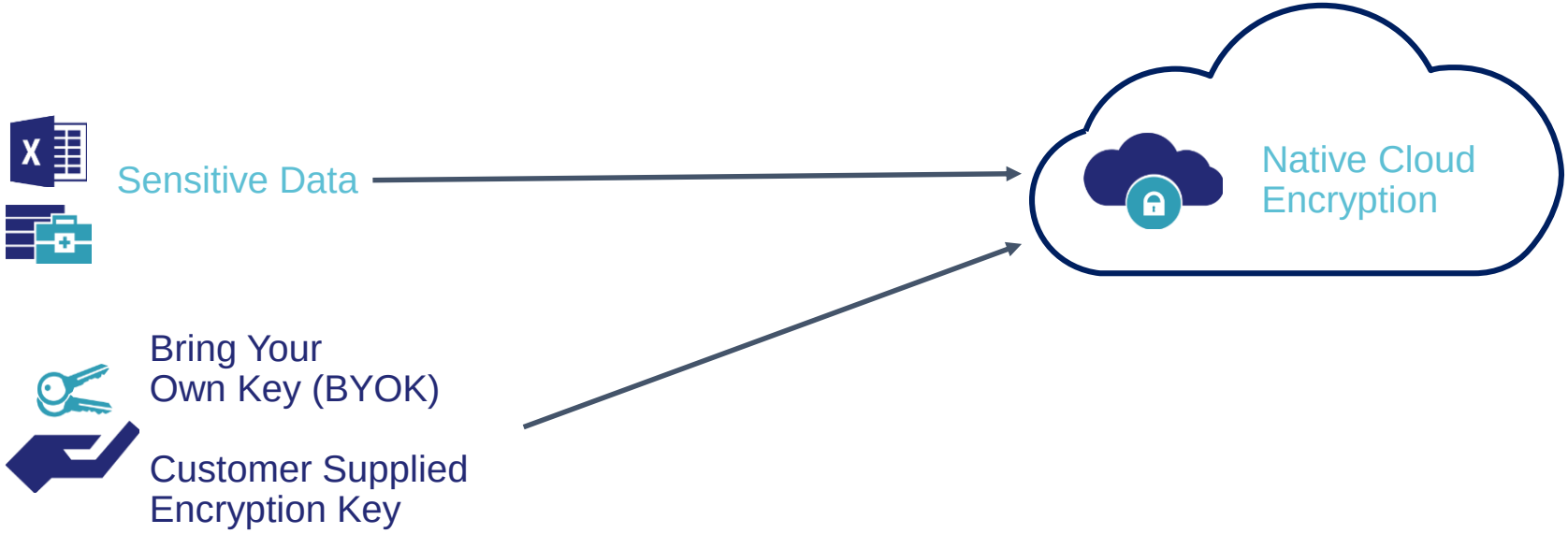
rozwiązanie

Rozwiązania dwa:

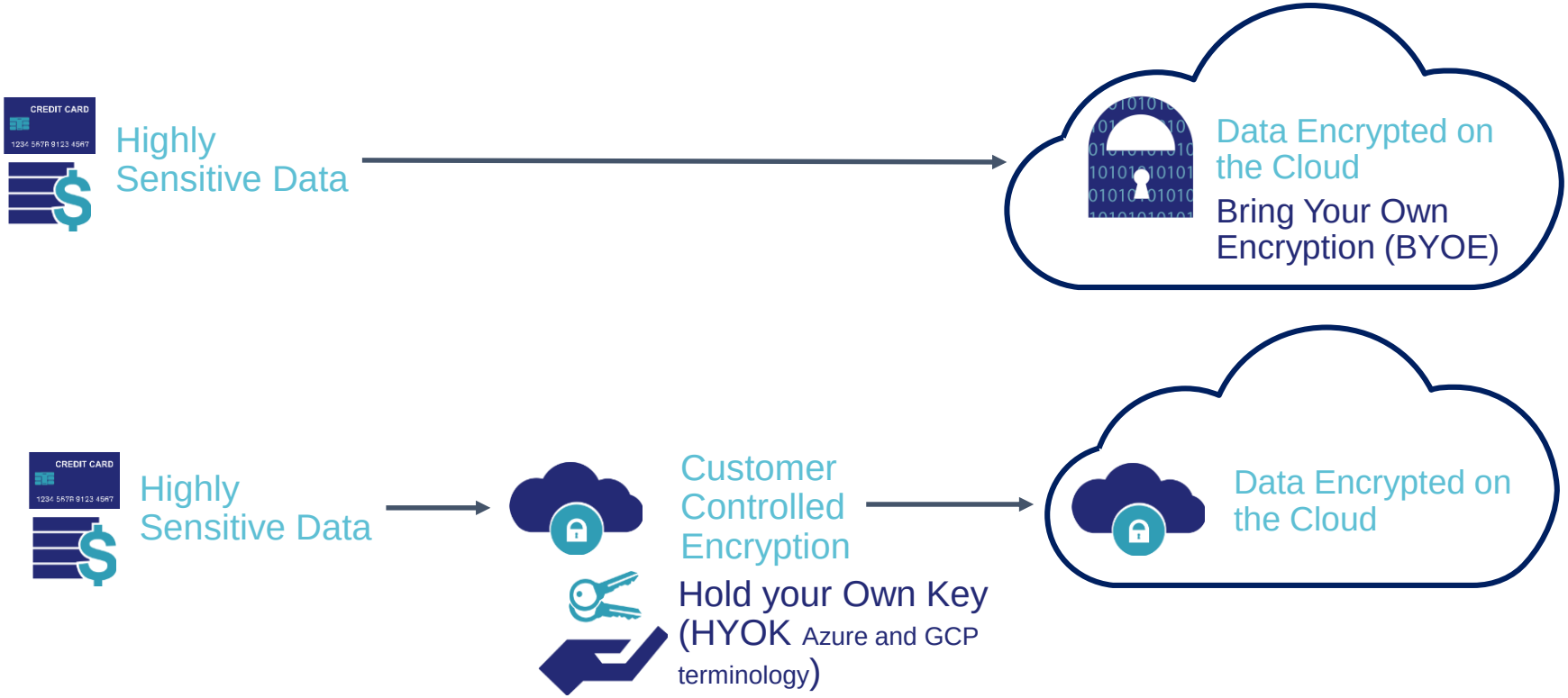
1. CM (z CCKM Embedded) w integracji z Azure (Storage) - BYOK

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

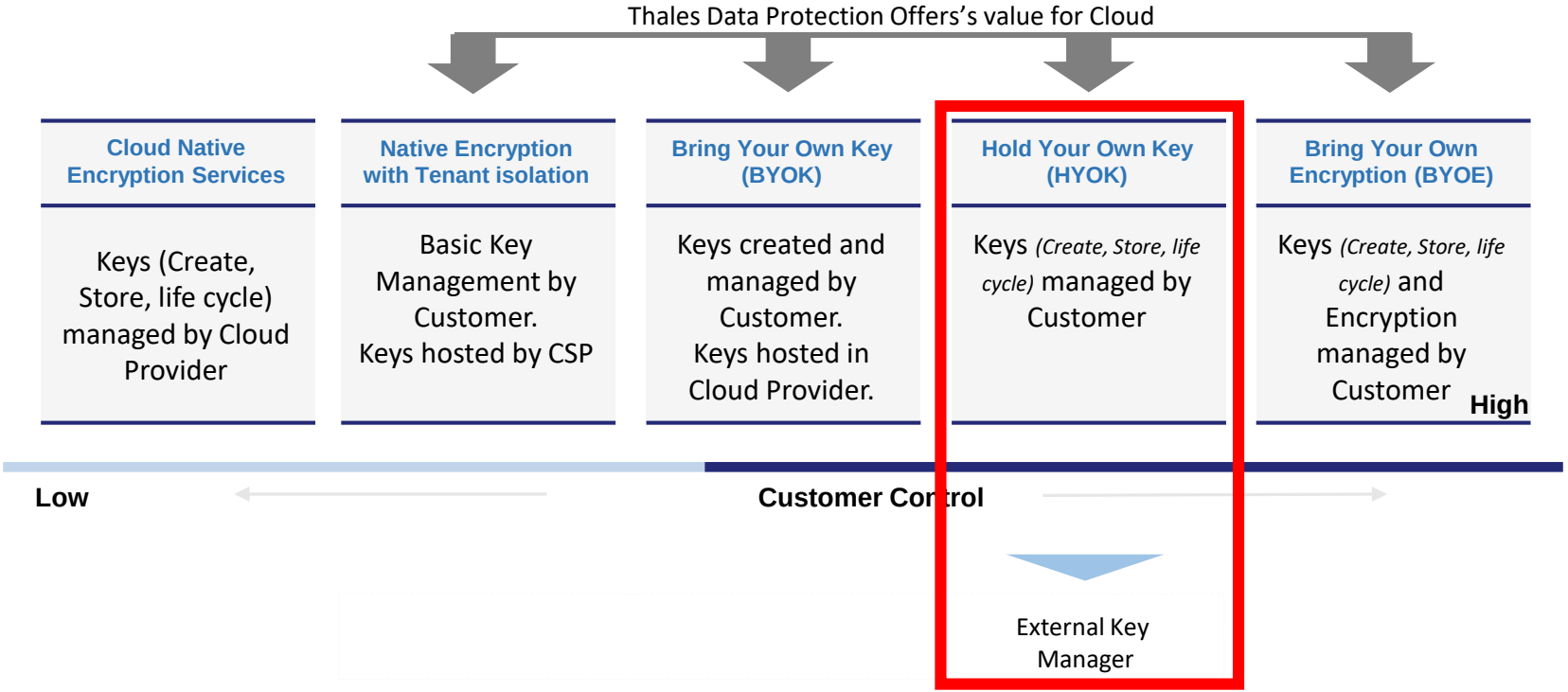
BYOK - Chmura dostarcza szyfrowanie, klient dostarcza klucze



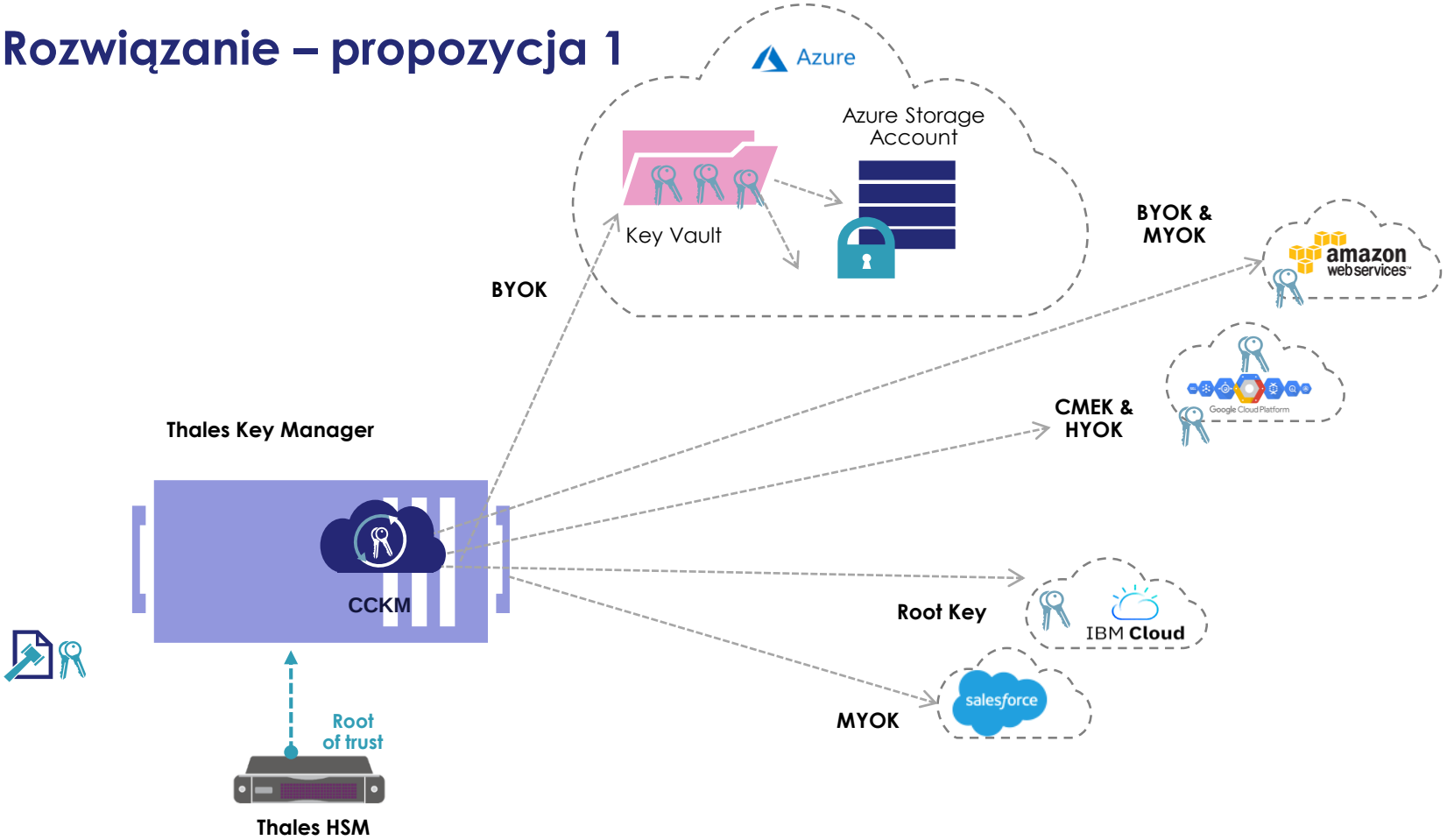
HYOE – Klient dostarcza szyfrowanie i klucze



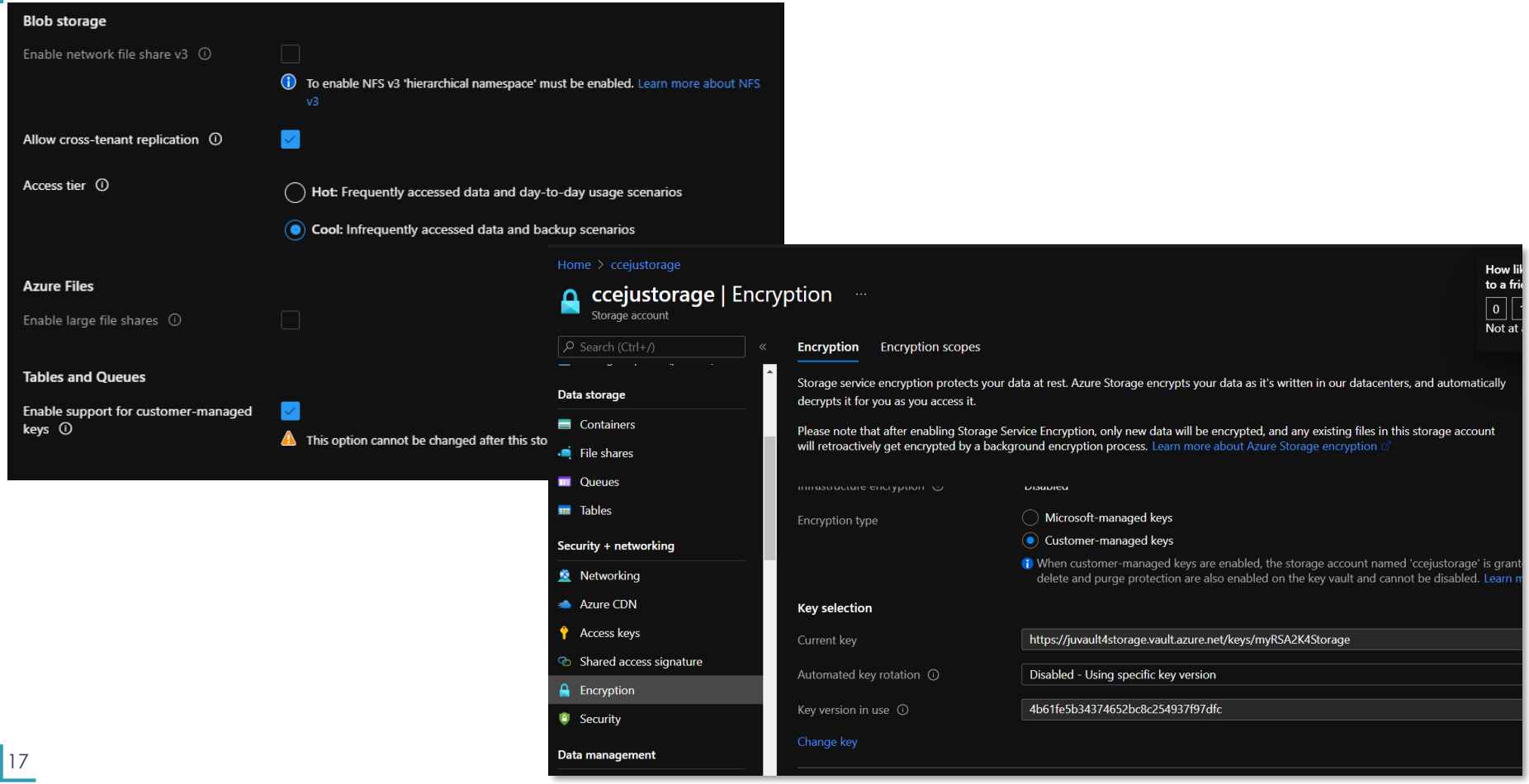
Encryption of Data at Rest in the Cloud / Levels of control



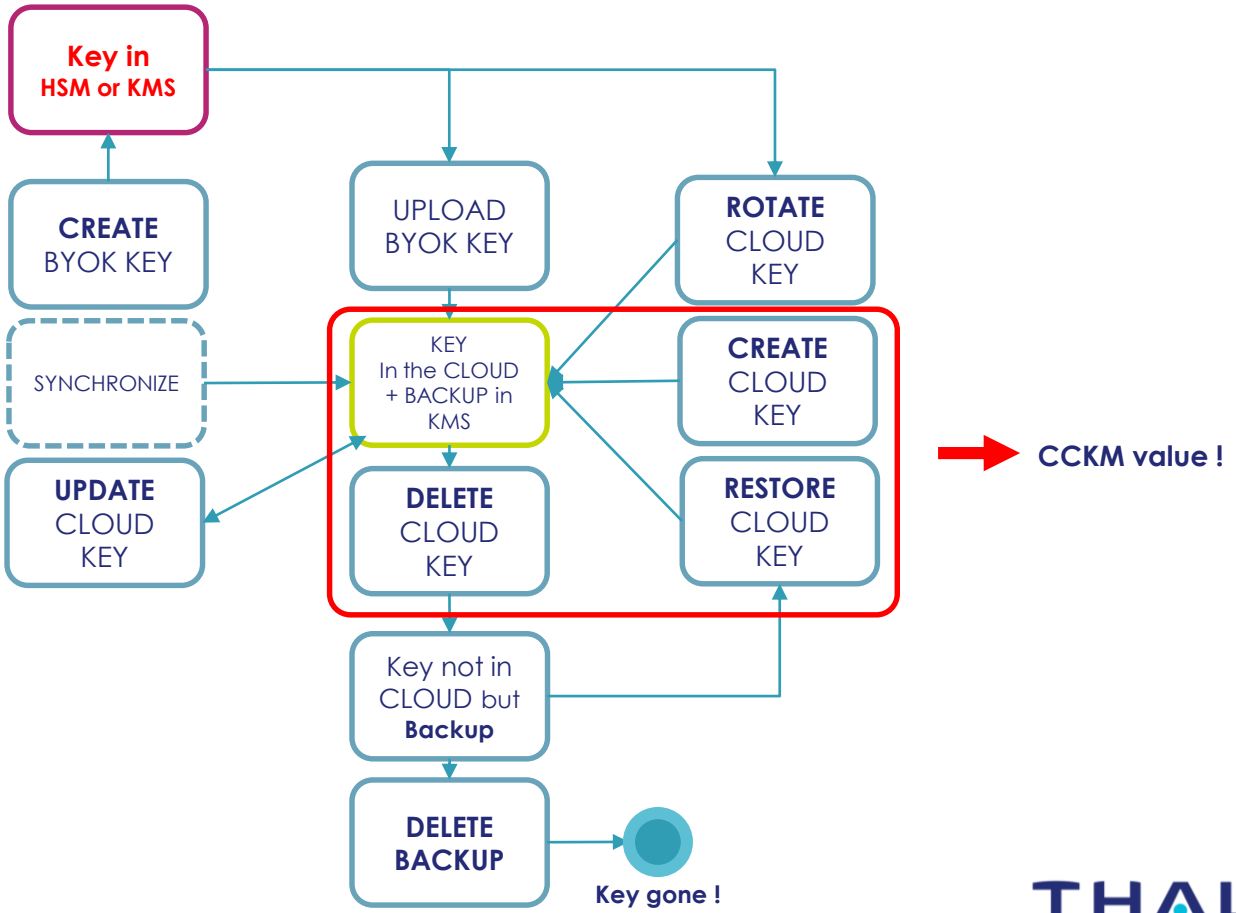
Rozwiązanie – propozycja 1



Tworzenie magazynu danych i jego szyfrowanie

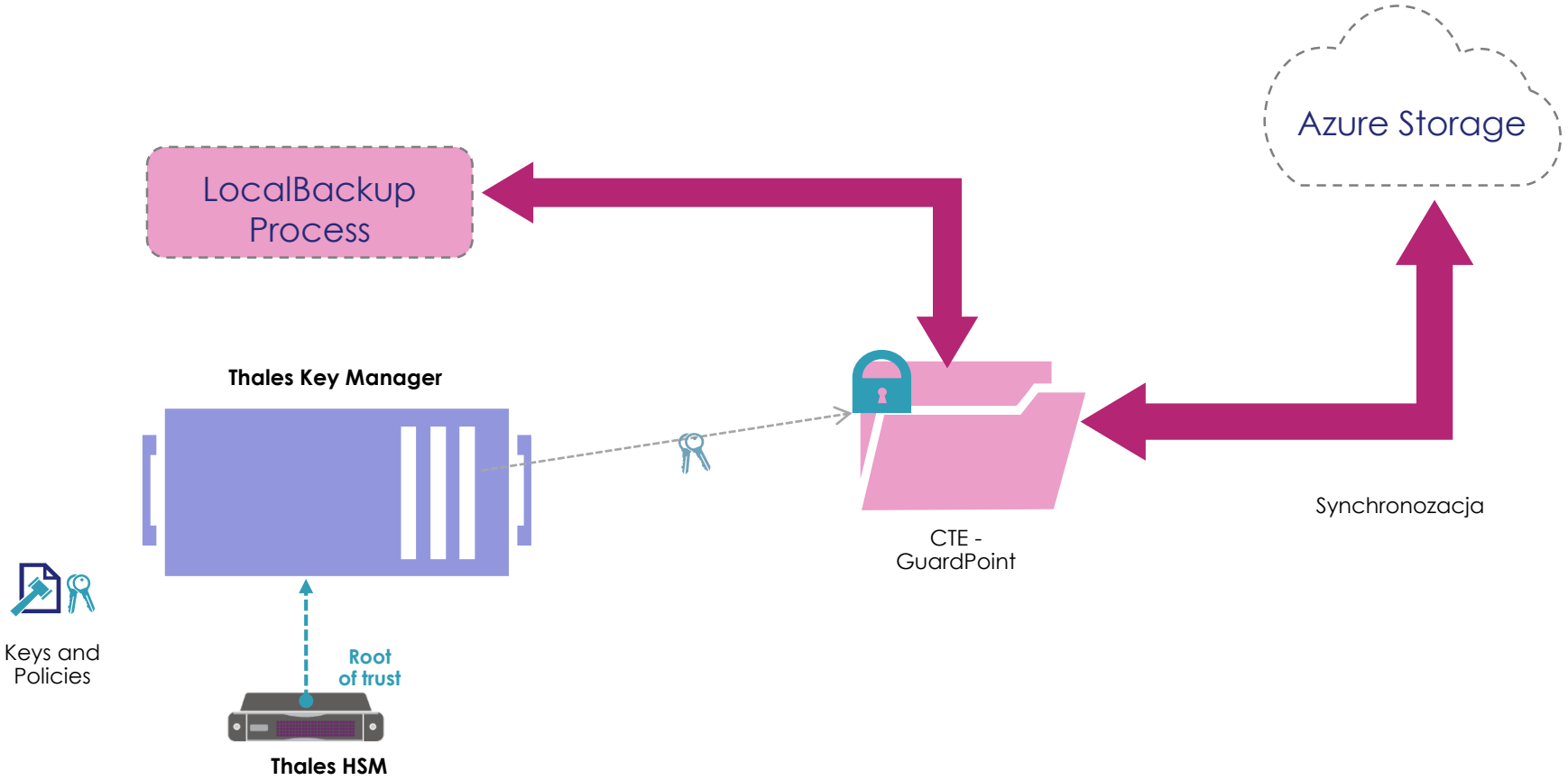


CCKM co w zasadzie daje? Disaster Recovery by design !



THALES

Rozwiązanie – propozycja 2 (HYOE)

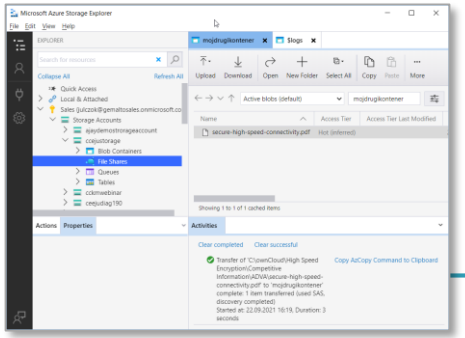


Rozwiązanie – propozycja 2

#	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, ???? Audit
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

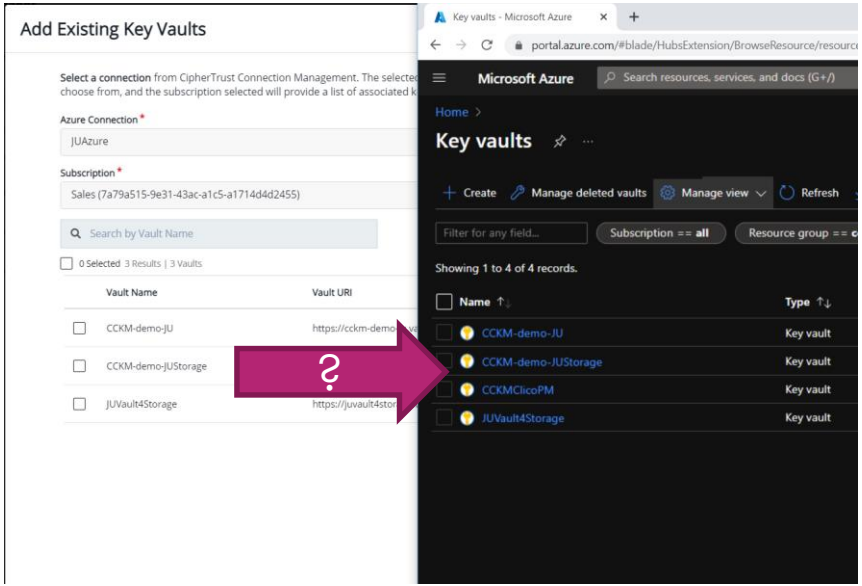


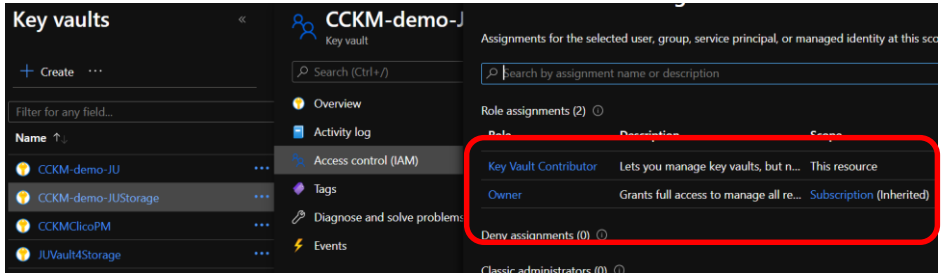
\myShare

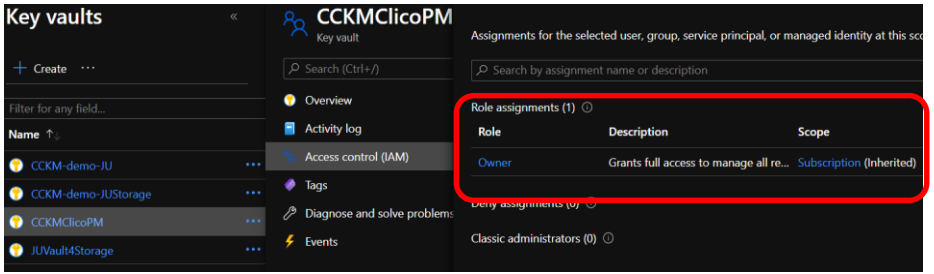
THALES

„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





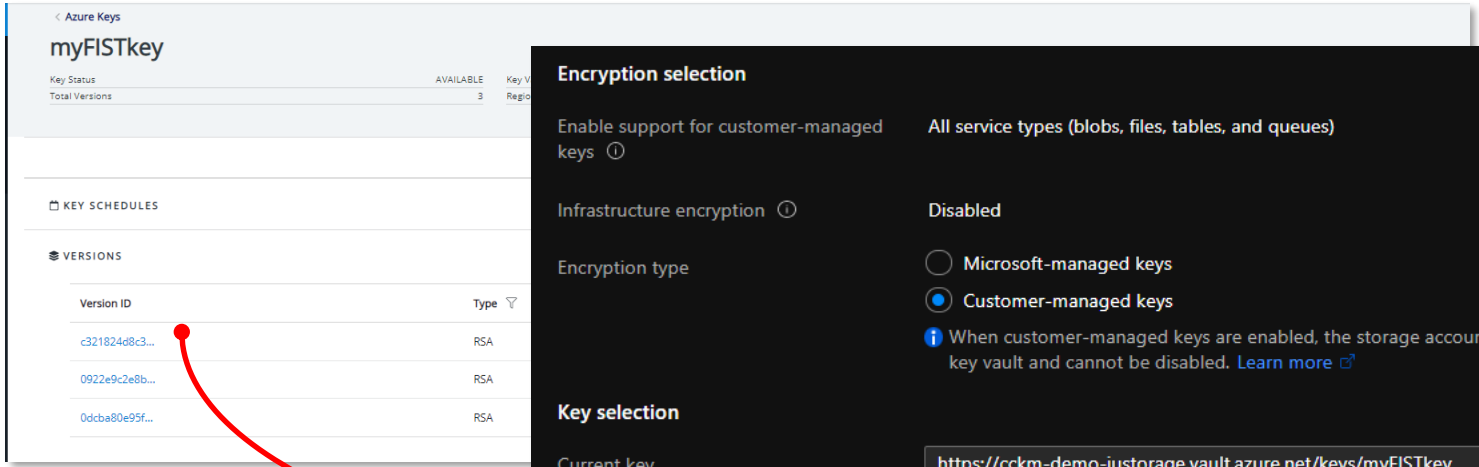


„Nauczki“, czyli *lessons learned #1/2*

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



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 is 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.thalesdocs.com/ctp/cm/latest/
- CCKM Azure – integracja: https://www.thalesdocs.com/ctp/cm/latest/admin/cckm_ag/azure/index.html
- CTE: https://www.thalesdocs.com/ctp/cte/Books/Online-Files/index-7.1.1.html

Zapraszamy także na...

THALES TRUSTED ACCESS SUMMIT, 5-6 October 2021