CryptoPanel

edycja #15

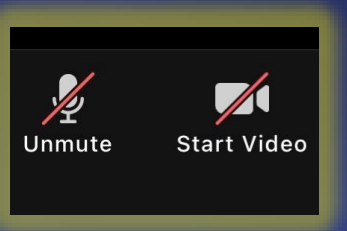
Już za moment zaczynamy...

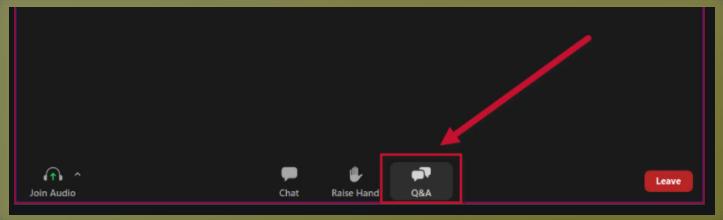
CryptoPanel

THALES

CLICO

CryptoPanel





CryptoPanel

edycja #13

Szyfrowanie w AWS.
Jak zabezpieczyć znajdujące się tam dane przy użyciu rozwiązań Thales?

CryptoPanel

dziś dyskutują i pokazują

Patryk Jonczyk

Security Specialist
Patryk.jonczyk@clico.pl
mob. +48 667 440 442

Piotr Majek

Security Specialist
piotr.majek@clico.pl
mob. +48 663 994 996

CryptoPanel

problem

co nas boli...

- Jesteśmy firmą korzystającą z usług chmurowych
- Nasza firma posiada centralę w Stanach Zjednoczonych, co wymusza konkretnego dostawcę chmury publicznej
- Nie obowiązuje nas nadzór Komisji Nadzoru finansowego, ale chcemy chronić dane zgodnie z wymogami dla organizacji tym nadzorem objętych
- Posiadamy zespół odpowiedzialny za bezpieczeństwo danych i korzystamy już z HSM Thales

- Chcemy się dowiedzieć jakie są dostępne możliwości (modele) zarządzania kluczami w AWS
- Chcemy wykorzystać istniejącą infrastrukturę opartą o HSM, dodając niezbędne komponenty pozwalające na integrację z chmurą publiczną
- Dążymy do zwiększenia bezpieczeństwa z możliwością regulowania dostępu do danych zabezpieczonych z użyciem zewnętrznie zarządzanych kluczy

CryptoPanel

rozwiązanie

Statystyki chmur – trochę danych

Cloud Migration Market Statistics

- A subsidiary of Amazon, AWS currently holds 31 percent of the market followed by Microsoft Azure at 20 percent and Google Cloud at seven percent. [2]
- Its market value is estimated at more than $90 billion 18. [2]
- Looking at the global cloud market by region, North America is leading the race, with 61 percent of the market total in 2020. [2]
- That's three times the size of the second largest market, Western Europe, which has 21 percent of the market total. [2]
- With an average compound annual growth rate of 21 percent, this market is predicted to grow to $223.98 billion in revenue by 2028.15. [2]
- In 2019, a CAGR
  - Amazon Web Services has the largest cloud computing market share at 32%. [1]
  - The average spendings have risen by 35.8% since 2016 which attests to the growing interest of enterprises in the cloud computing market. [1]
  - This process will boost the influence of the top industry vendors and grant them control over 75% of the market. [1]
  - Currently, the top five "only" account for about 50% of the cloud market. [1]
  - Cloud computing statistics place Microsoft Azure second with 16.8% of the global cloud market. [3]

Statystyki chmur – trochę więcej danych

Cloud Migration Adoption Statistics

- Azure was the only provider to increase their adoption rate. [8]
- YoY. Google Cloud Platform showed the highest percentage of experimentation , which tends to drive more adoption in the future. [8]
- Platformasa Service grew in adoption to 56% by 2020. [1]
- Platformasa Service grew in adoption to 56%. [1]
- In 2020, Amazon Web Services had a 76% share of enterprise cloud adoption, followed by Microsoft Azure with a 69% share and Google Cloud with a 34% share. [6]

- While free platforms like Dropbox and iCloud continue to excel as the most popular free file storage services, Amazon Web Services appear to be the clear winner according to cloud computing stats in 2023. [1]
- AWS holds the next largest percentage at 32%. [1]
- Cloud computing actually started in the US and they have been leading the way since 2015, according to cloud computing statistics by country. [1]

Źródło: Cloud Migration Statistics 2022 - Everything You Need to Know (webinarcare.com)

O co chodzi z tym KNF?

UKNF | URZĄD KOMISJI NADZORU FINANSOWEGO

Warszawa, 23 stycznia 2020 r.

Komunikat Urzędu Komisji Nadzoru Finansoweg
dotyczący przetwarzania przez podmioty nadzorowane informacji w c
publicznej lub hybrydowej

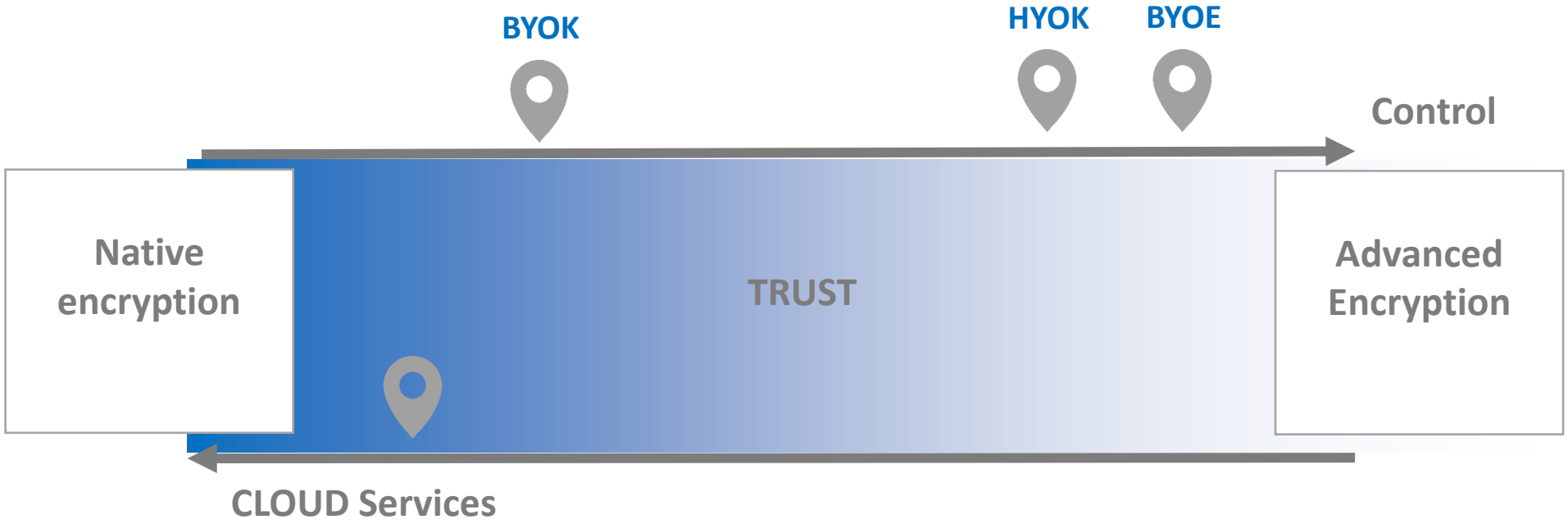
14) **szyfrowanie „at rest”** przechowywanych kopii plików);

7. Kryptografia

7.1. Podmiot nadzorowany powinien zapewnić, że informacje przetwarzane w chmurze obliczeniowej są szyfrowane zgodnie z zasadami określonymi w niniejszym komunikacie. W szczególności podmiot nadzorowany powinien upewnić się, że:

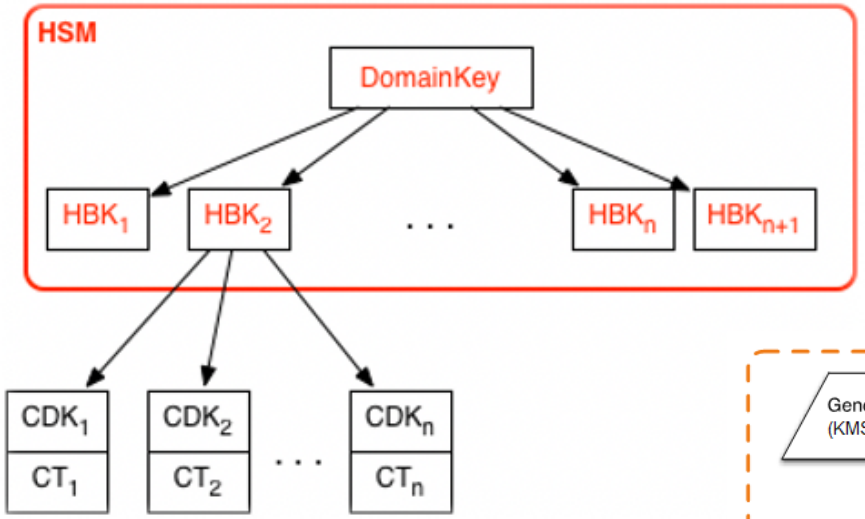
a) posiada dostęp do szczegółowych i aktualnych instrukcji konfiguracji usług chmury obliczeniowej oraz metod weryfikacji poprawności ich konfiguracji i działania, w szczególności w zakresie szyfrowania przetwarzanych informacji;
b) zapewnia dostateczne kompetencje w celu realizacji poprawnej konfiguracji usług chmury obliczeniowej, zgodnie z wytycznymi dostawcy usług chmury obliczeniowej, w tym pod kątem stosowania szyfrowania przetwarzanych informacji;
c) używa dedykowanych lub zalecanych przez dostawcę usług chmury obliczeniowej ustawień konfiguracyjnych podnoszących bezpieczeństwo świadczonych usług chmury obliczeniowej;
d) informacje prawnie chronione przetwarzane w chmurze obliczeniowej są szyfrowane zarówno „at rest” jak i „in transit”.

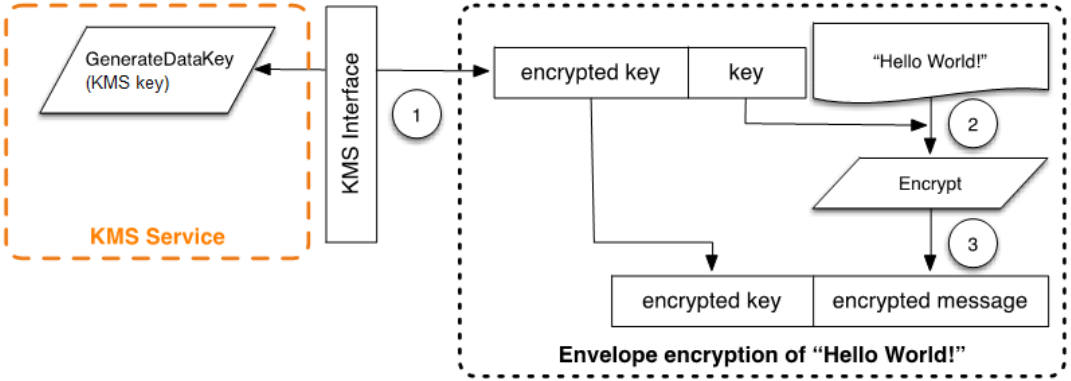
Bezpieczeństwo i zaufanie



Rozwiązanie – ponownie CipherTrust Manager!

Jak działa KMS w AWS?





Jak działa XKS?

Dlaczego CCKM dla obsługi XKS w AWS?

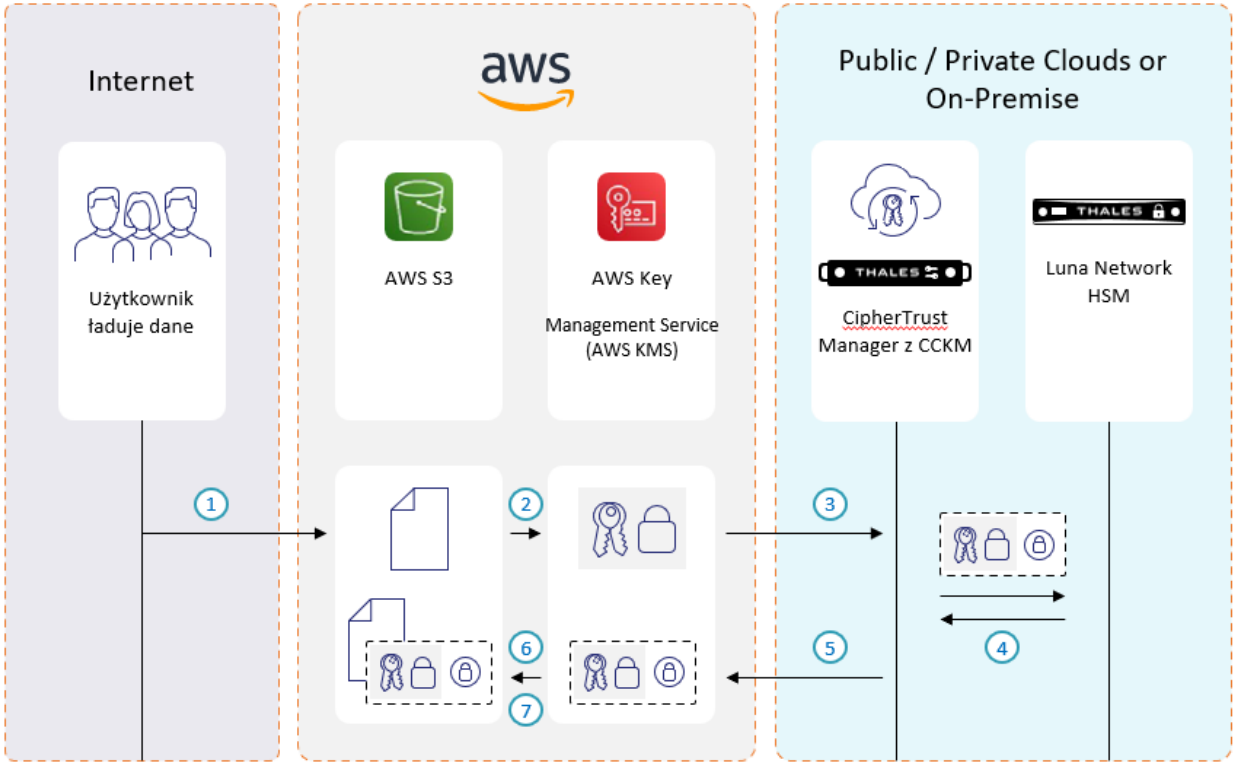
Z pojedynczej konsoli CCKM możesz zarządzać kluczami w modelu BYOK, XKS (HYOK), AWS Native i kluczami w AWS CloudHSM.

Wybór pomiędzy CipherTrust Manager lub HSMem Luna jako źródłem kluczy

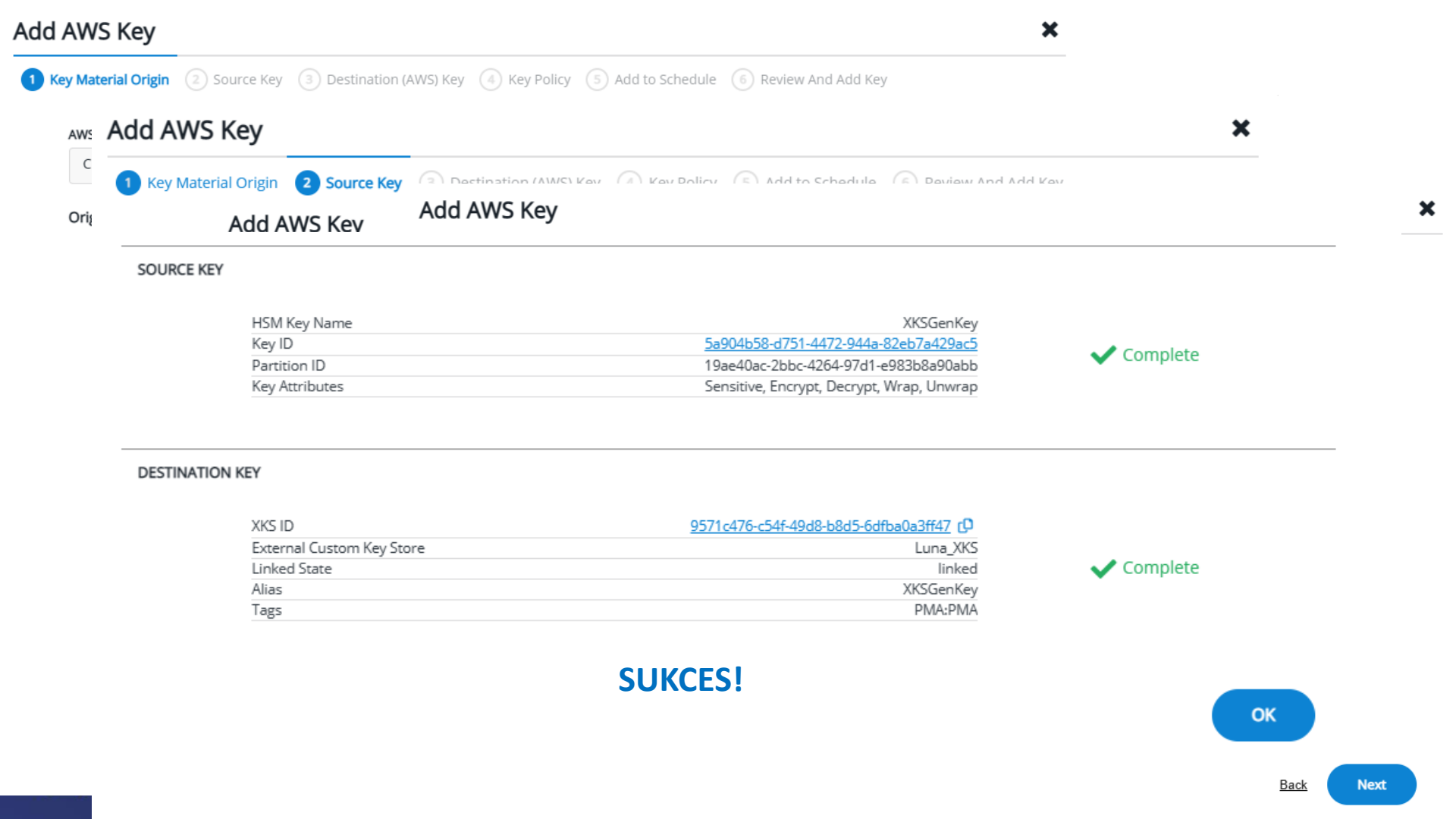
Zapewnienie zgodności z regulacjami takimi jak na przykład RODO lub wymogami KNF

Zarządzaj dostępem do kluczy dla usług w środowisku chmurowym lub hybrydowym

XKS – krok po kroku



1. Użytkownik ładuje obiekt do AWS S3.
2. AWS S3 wysyła zapytanie do AWS KMS aby wygenerować klucz
3. AWS KMS przesyła zaszyfrowane dane do CCKM dla podwójnego szyfrowania
4. CCKM weryfikuje autentyczność zapytania używając dostępów konta. Klucz XKS jest użyty przez CM lub Lunę do podwójnego szyfrowania klucza zabezpieczającego dane (uff ;))
5. CCKM zwraca podwójnie zaszyfrowany klucz zabezpieczający dane do KMS w AWS
6. KMS przesyła klucz i jego odszyfrowaną wartość do S3 w AWS
7. S3 szyfruje dane za pomocą jawnych bitów klucza, zachowuje jego formę zaszyfrowaną i usuwa z pamięci bity klucza


Add AWS Key
1 Key Material Origin
2 Source Key
3 Destination (AWS) Key
4 Key Policy
5 Add to Schedule
6 Review And Add Key
Add AWS Key
1 Key Material Origin
2 Source Key
Add AWS Kev
Add AWS Key
SOURCE KEY
HSM Key Name XKSGenKey
Key ID 5a904b58-d751-4472-944a-82eb7a429ac5
Partition ID 19ae40ac-2bbc-4264-97d1-e983b8a90abb
Key Attributes Sensitive, Encrypt, Decrypt, Wrap, Unwrap
Complete
DESTINATION KEY
XKS ID 9571c476-c54f-49d8-b8d5-6dfba0a3ff47
External Custom Key Store Luna_XKS
Linked State linked
Alias XKSGenKey
Tags PMA:PMA
Complete
SUKCES!
OK
Back
Next

Szyfrujmy! Na

Create bucke

Buckets are containers fo

General configur

Bucket name

pmabucket4encrypti

Bucket name must be glob

AWS Region

EU (Stockholm) eu-n

Copy settings from exi

Only the bucket settings i

Choose bucket

Crypto

Object Ownership Info

Control ownership of objects written to this bucket determines who can specify access to objects.

ACLs disabled (recommended)

All objects in this bucket are owned by this a Access to this bucket and its objects is specif only policies.

Object Ownership

Bucket owner enforced

Block Public Access settings for t

Public access is granted to buckets and objects thro ensure that public access to this bucket and its obje and its access points. AWS recommends that you tu applications will work correctly without public acces customize the individual settings below to suit your

Block *all* public access

Turning this setting on is the same as turning o

Block public access to buckets and

S3 will block public access permissions app ACLs for existing buckets and objects. This using ACLs.

Block public access to buckets and

S3 will ignore all ACLs that grant public ac

Block public access to buckets and

S3 will block new bucket and access point existing policies that allow public access to

Block public and cross-account acce policies

S3 will ignore public and cross-account acc objects.

Default encryption Info

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption key type Info

- Amazon S3-managed keys (SSE-S3)
- AWS Key Management Service key (SSE-KMS)

AWS KMS key Info

- Choose from your AWS KMS keys
- Enter AWS KMS key ARN

Available AWS KMS keys

arn:aws:kms:eu-north-1:813472922977:key/c5d3... ▼ | Create a KMS key

Bucket Key

When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. Learn more

- Disable
- Enable

▸ Advanced settings

After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.

Cancel | Create bucket

Amazon S3 > Buckets > pmabucket4encryption > Upload

Upload Info

Add the files and folders you want to upload
S3 REST API. Learn more

Drag and drop files and fold

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<Error>
  <Code>KMS.DisabledException</Code>
  <Message>arn:aws:kms:eu-north-1:813472922977:key/c5d3e53c-a3a9-4211-b4a7-04f339eb7125 is disabled</Message>
  <RequestId>988DQB9HTMT07F8W</RequestId>
  <HostId>97Gc4V5YdumY/tZDDrE2V6i2N1mKNM2mS/aACroddY05A/I/OrQsu+edy95ify4hWgR3uf+Fcj8=</HostId>
</Error>
```

Files and folders (4 Total, 8.7 M

All files and folders in this table will be uploaded

Find by name

Name	Fo
007-000465-001_K7_CC_User_Guidance_Part2_AGD_OPE_RevF (1).pdf	-
007-000466-001_K7_CC_User_Guidance_Part3_AGD_OPE_RevE.pdf	-
007-000467-001_K7_CC_User_Guidance_Part4_AGD_OPE_RevD.pdf	-
007-013968-001_K7_CC_User_Guidance_Part1_AGD_PRE_ReVE (1).pdf	-

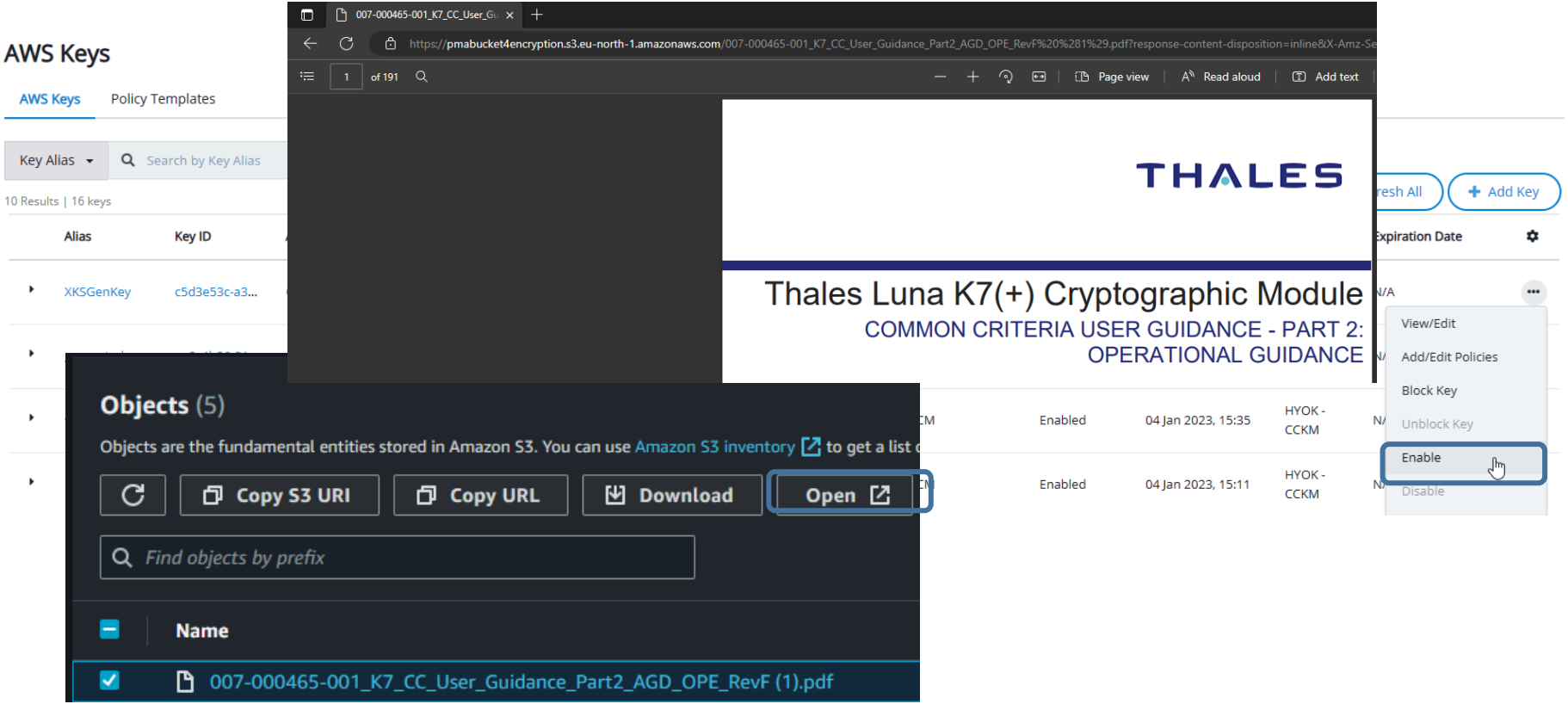
Customer managed keys (5)

Filter keys by properties or tags

Aliases	Key ID	Status
FirstXKS	0b3e6ae8-a260-4487-89ca-ef591e954a5a	Enabled
FirstKeyFromCM	933ddb8f-f0a9-4a58-8498-4b1689b785dd	Enabled
generated_on-CM_availabe_in_AWS	aa8c4b86-31ac-4cad-957e-7cdb169962c6	Enabled
XKSGenKey	c5d3e53c-a3a9-4211-b4a7-04f339eb7125	Disabled
wygenerowany_w_CM	e396561c-58ce-4916-8578-1581960fa134	Enabled

application/pdf 2.6 MB

Jak dane odblokować?



Wiela to w tym AWS kosztuje i jakie obsługuje usługi?

Quota name	Default value
AWS KMS keys	100,000
Aliases per KMS key	50
Grants per KMS key	50,000
Key policy document size	32 KB (32,768 bytes)
Custom key stores	10

Nie każda usługa (niestety) wspiera XKS!

[Features | AWS Key Managem

Amazon Connect Voice ID	Amazon Lex	Amazon Simple Notification Service (SNS)	AWS Glue DataBrew
Amazon Connect Wisdom	Amazon Lightsail[1]	Amazon Simple Queue Service (SQS)	AWS IoT SiteWise
Amazon DocumentDB	Amazon Location Service	Amazon Textract	AWS Lambda
Amazon DynamoDB	Amazon Lookout for Equipment	Amazon Timestream	AWS License Manager
Amazon DynamoDB Accelerator (DAX)[1]	Amazon Lookout for Metrics	Amazon Transcribe	AWS Network Firewall
Amazon EBS	Amazon Lookout for Vision	Amazon Translate	AWS Proton
Amazon EC2 Image Builder	Amazon Macie	Amazon WorkMail	AWS Secrets Manager
Amazon EFS	Amazon Managed Blockchain	Amazon WorkSpaces	AWS Snowball
Amazon Elastic Container Registry (ECR)	Amazon Managed Service for Prometheus	Amazon WorkSpaces Web	AWS Snowball Edge
Amazon Elastic Kubernetes Service (EKS)	Amazon Managed Streaming for Kafka (MSK)	AWS Audit Manager	AWS Snowcone
Amazon Elastic Transcoder	Amazon Managed Workflows for Apache Airflow (MWAA)	AWS Application Cost Profiler	AWS Snowmobile
Amazon ElastiCache	Amazon MemoryDB	AWS Application Migration Service	AWS Storage Gateway
Amazon EMR	Amazon Monitron	AWS App Runner	AWS Systems Manager
Amazon EMR Serverless	Amazon MQ	AWS Backup	AWS X-Ray
Amazon FinSpace	Amazon Neptune	AWS Certificate Manager[1]	
Amazon Forecast	Amazon Nimble Studio	AWS Cloud9[1]	
Amazon Fraud Detector	Amazon OpenSearch	AWS CloudHSM[2]	

CryptoPanel

podsumowanie

Podsumowanie, czyli co potrzeba…

Ile licencji CCKM? Tyle ile kont w AWS!

Cloud Service Provider	aws	Azure
CCKM Cloud UNITS required per the following	Accounts	Subscriptions
Key Management System	AWS KMS	Azure Key Vault

CCKM, Cloud Units, Term Based, Enhanced Support **12,480.00**

Zalecamy klaster CM – to już nie przelewki!

Virtual CipherTrust Manager,k170v,Perpetual License **16,640.00**

CCKM łączy klucze zarządzane w modelu HYOK!

- CCKM pozwala na zarządzanie kluczami w modelu HYOK – zarówno AWS XKS, jak i w innych chmurach!

A dzięki CCKM - XKS i bezpieczeństwo danych idą ręka w rękę!

CryptoPanel

CryptoPanel

A teraz quiz

https://forms.office.com/e/X8Jgej7hhX

THALES