CryptoPanel

edycja #18

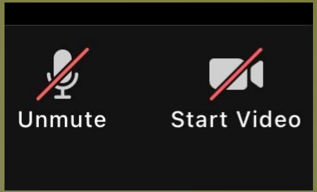
za chwilę zaczynamy...

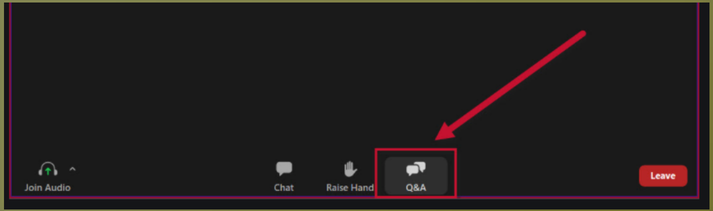
CryptoPanel

THALES

CLICO

CryptoPanel





CryptoPanel

edycja #18

Centralne repozytorium oraz zarządzanie poświadczeniami i kluczami szyfrującymi dla rozwiązań OT i IoT

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

TEST WIEDZY #18

Centralne repozytorium oraz zarządzanie poświadczeniami i kluczami szyfrującymi dla rozwiązań OT i IoT

CryptoPanel

problem

co nas boli...

Jesteśmy dostawcą mediów. Wykorzystujemy rozwiązania klasy OT.

Eksploatujemy autorskie rozwiązanie klasy Head End System (HES) dla sieci inteligentnych liczników

- 500 000+ liczników, 20% z odczytem on-line
- 7000 koncentratorów danych z liczników z odczytem on-line
- do 2030 plan na 1000 000 liczników on-line

Wyprowadzanie centralnego repozytorium certyfikatów, kluczy szyfrujących i sekretów poza system HES

- Ustawa o prawie energetycznym.
- Zarządzanie tym kto generuje i dostarczą klucze szyfrujące do HES.
- Wykorzystanie w innych systemach (poza HES).

...poszukujemy kompletnego rozwiązania

- **PKI** na potrzeby OT
- dostarczanie **sekretów** do systemu HES
- dostarczanie **kluczy** (3xAES) dla systemu HES do zabezpieczania połączenia zdalnego do liczników
- **zarządzenie** kluczami w ramach OT (import, rotacja, itp..)

…ale priorytetem jest ochrona i dostarczanie kluczy

…dostępność na poziomie 99,95%

- współpraca z naszym: HAproxy

…zasoby: 2xDC wiele styków do sieci liczników

…posiadamy własnych programistów

…preferujemy dedykowane rozwiązanie sprzętowe

…mile widziany FIPS ale nie ma konieczności

W zasadzie co to jest to „OT” i „IT”?

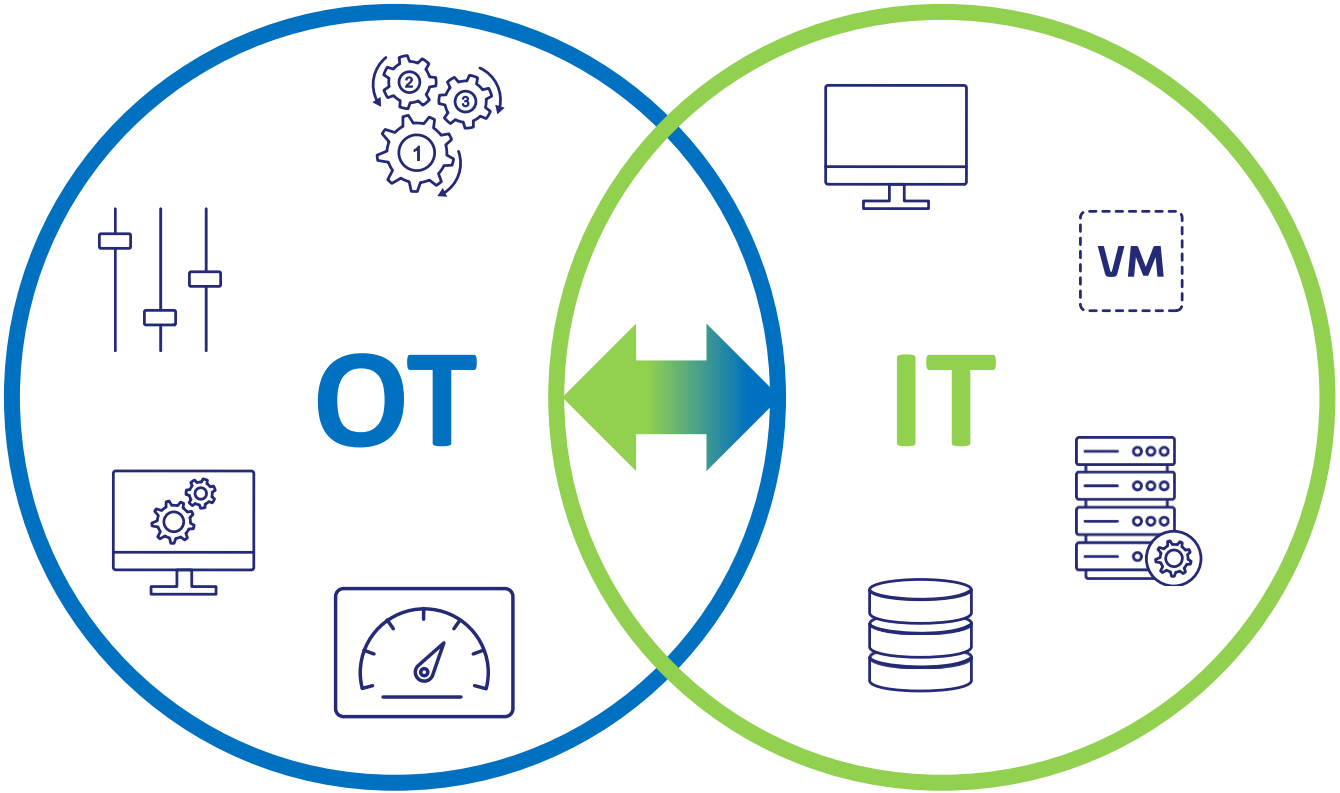
OT (technologia operacyjna) odnosi się do **sprzętu i oprogramowania** używanego do zmiany, monitorowania lub **sterowania fizycznymi urządzeniami,** procesami i zdarzeniami w fabryce lub zakładzie produkcyjnym.

IT (technologia informacyjna) **odnosi się do** wszystkiego, co dotyczy **technologii komputerowej**, w tym **sprzętu i oprogramowania**.

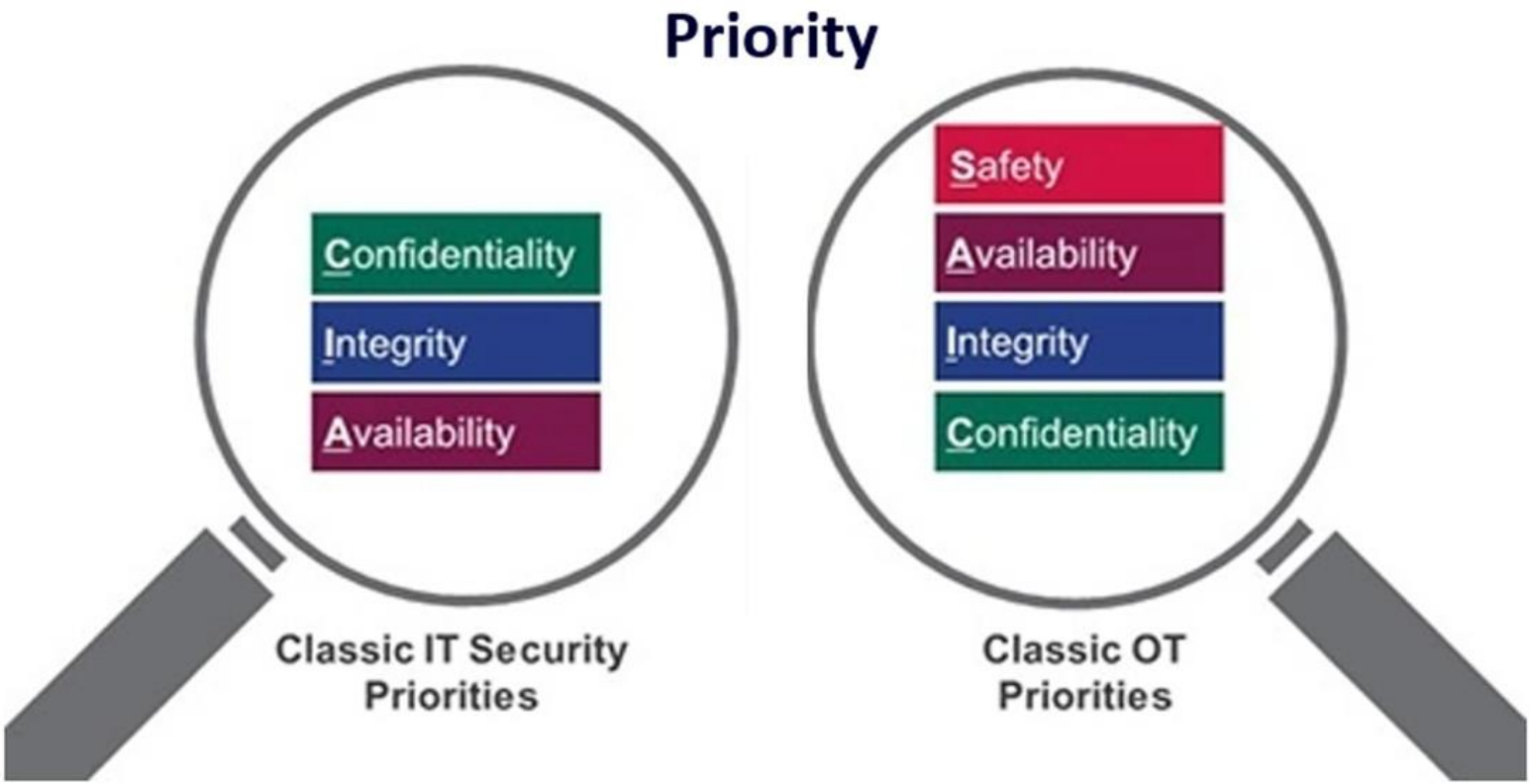
IoT (internet rzeczy) - koncepcja, wedle której jednoznacznie **identyfikowalne przedmioty** mogą pośrednio albo bezpośrednio gromadzić, przetwarzać lub **wymieniać dane** za pośrednictwem **sieci** komputerowej.

IIoT to przemysłowy internet rzeczy i jest podkategorią IoT. Odnosi się do **technologii IoT** wykorzystywanych w **konfiguracjach przemysłowych.**

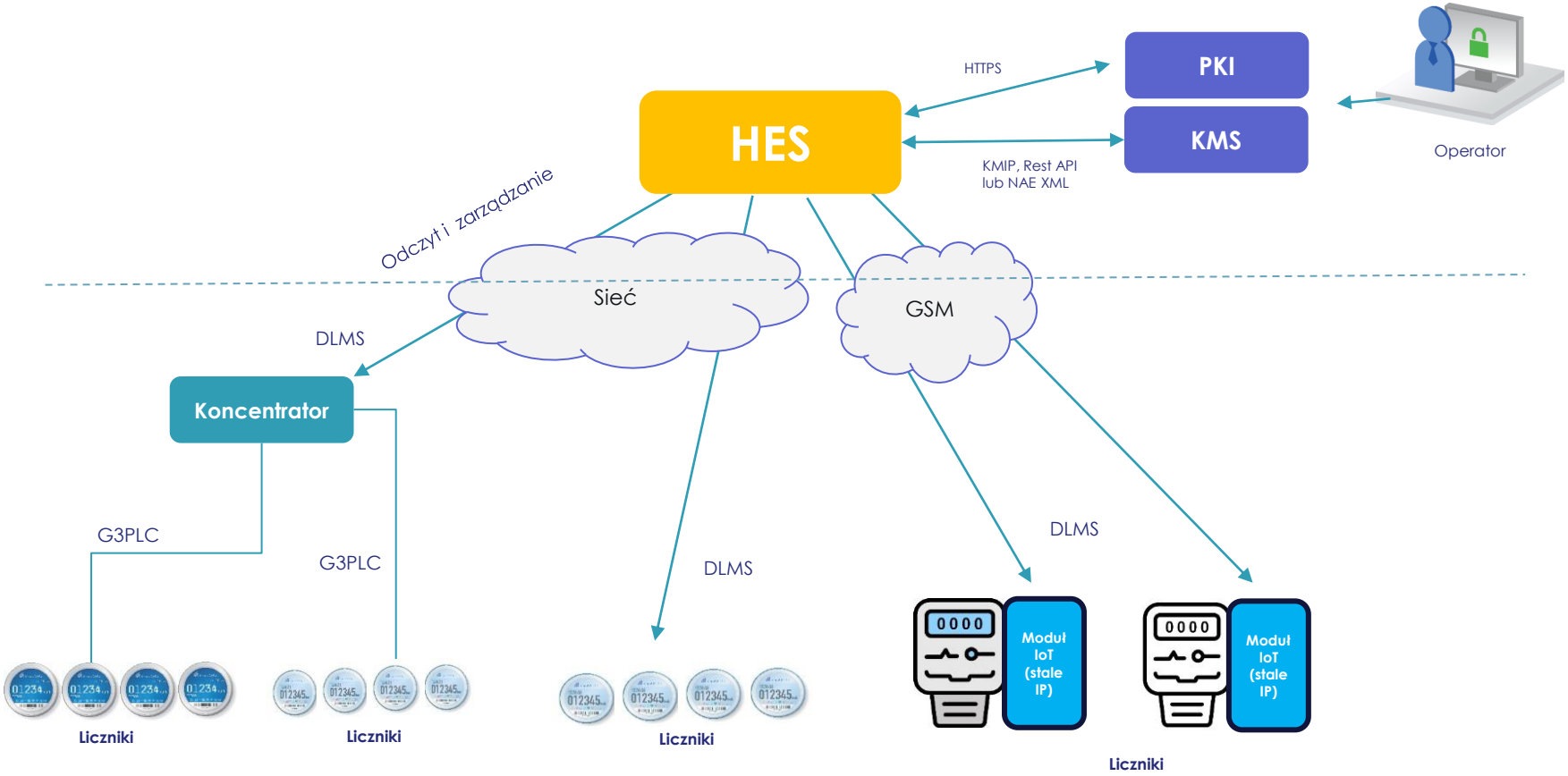
Źródła: https://www.aloxy.io/publications/introduction-to-industrial-iot
https://www.copadata.com/pl/product/platform-editorial-content/co-to-jest-iot-oraz-iiot/
https://pl.wikipedia.org/wiki/Internet_rzeczy



Główna różnica między rozwiązaniami OT a rozwiązaniami IT polega na tym, że urządzenia **OT kontrolują świat fizyczny,** podczas gdy systemy **IT zarządzają danymi**.


Priority
Confidentiality
Integrity
Availability
Classic IT Security Priorities
Safety
Availability
Integrity
Confidentiality
Classic OT Priorities

Architektura problemu



THALES

CryptoPanel

rozwiązanie

Rozwiązanie to:

1. Wykorzystanie urządzenia CipherTrust Manager (k470) jako repozytorium kluczy i sekretów

2. Wdrożenie „wysokodostępne” (HA + odpowiednie wsparcie)

3. Zastosowanie Rest API do importu, generowania, pobierania kluczy (do HES)

Rozwiązanie – pojemność

„500 000+ liczników, 20% z odczytem on-line
7000 koncentratorów danych z liczników z odczytem on-line
do 2030r plan na 1000 000 liczników on-line"

<u>Dziś:</u>
500 000 x 0,2 +7000 = 107 000 punktów =>
3 obiekty (2x AES256 + 1 ID) = **321 000** obiektów…
a zatem **k470** lub **k470v**

<u>2030r (to za 7 lat!):</u>
1 000 000 x3 = 3 000 000 - > czyli k470**v** (brak twardych limitów)

lub podział kluczy na grupy i przetrzymywanie w oddzielnych KMS

lub <a jaki wy macie pomysł? To pytanie do uczestników>

CipherTrust Manager Features

Features	Virtual Appliances		Physical Appliances	
	k170v	k470v	k470	k570
Administrative Interfaces	Management Console, REST API, kscfg (system configuration), (ksctl (Command Line Interface)			
Network Management	SNMP v1, v2c, v3, NTP, Syslog-TCP			
Monitoring	Prometheus, Splunk			
API Support	REST, NAE-XML, KMIP, PKCS#11, JCE, .NET, MCCAPI, MS CNG			
Secure Authentication	Local User , AD/LDAP, LDAPS, Certificate based authentication, Supports Open ID Connect (OIDC)			
System Formats	RFC-5424, CEF, LEEF			
Supported HSMs for Root of Trust	Luna Network HSM, Luna T-Series Network HSM, Luna Cloud HSM, AWS Cloud HSM, Azure Dedicated HSM, IBM Cloud HSM, IBM Cloud Hyper Protect Crypto Services Cloud HSM, nShield Network HSM	Luna Network HSM, Luna T-Series Network HSM, Luna Cloud HSM, AWS Cloud HSM, Azure Dedicated HSM, IBM Cloud HSM, IBM Cloud Hyper Protect Crypto Services Cloud HSM, nShield Network HSM	Luna Network HSM, Luna T-Series Network HSM, Luna Cloud HSM, AWS Cloud HSM, Azure Dedicated HSM, IBM Cloud HSM, IBM Cloud Hyper Protect Crypto Services Cloud HSM, nShield Network HSM	**Built-in HSM**, Luna Network HSM, Luna T-Series Network HSM, Luna Cloud HSM, AWS Cloud HSM, Azure Dedicated HSM, IBM Cloud HSM, IBM Cloud Hyper Protect Crypto Services Cloud HSM, nShield Network HSM
Automated Deployment Support	Yes (via Terraform, Cloud-Init)	Yes (via Terraform, Cloud-Init)	No	Yes (via Secure Transport Mode)
Maximum Number of Keys	Tested up to 1M Keys (more possible with appropriately sized virtual environments)	Tested up to 1M Keys (more possible with appropriately sized virtual environments)	1 Million Keys	1 Million Keys
Maximum Domains (multi-tenancy)	100	1000	1000	1000
FIPS Support	FIPS 140-2 L1 (Certificate #4430)			
	Integrates with an external FIPS Certified Physical or Cloud HSM as Secure Root of Trust			Embedded PCI-HSM FIPS 140-2 Level 3 certified – password and multi-factor (PED) (Certificate #4090)

THALES

Rozwiązanie – dostęp do kluczy

Rest API

- https://thalesdocs.com/ctp/cm/2.11/admin/cm_admin/rest-api/index.html

KMIP

- Wymaga licencji Flex Connector dla każdego klienta KMIP
- KMIP TLS version 1.0, 1.1, 1.2 (default minimum), 1.3
- https://www.thalesdocs.com/ctp/cm/latest/reference/kmip-ref/index.html

NAE-XML

- Wymaga licencji CDAP
- https://www.thalesdocs.com/ctp/cm/latest/reference/xml/inde.html

Dostępne REST APIs

Crypto

/v1/crypto/hide2
Format-preserving encrypt - post

/v1/crypto/unhide2
Format-preserving decrypt - post

/v1/crypto/encrypt
Encrypt - post

/v1/crypto/decrypt
Decrypt - post

/v1/crypto/mac
MAC - post

/v1/crypto/macv
MAC Verify - post

/v1/crypto/sign
Sign - post

/v1/crypto/signv
Sign Verify - post

/v1/crypto/encryptonite
Encryptonite - post

/v1/crypto/decryptonite
Decryptonite - post

/v1/vault/random
Random - get

Keys

/v1/vault/keys2/
List - get
Create - post

/v1/vault/keys2/{id}
Get - get
Update - patch
Delete - delete

/v1/vault/keys2/{id}/versions/
List versions - get
Create version - post

/v1/vault/keys2/{id}/destroy
Destroy - post

/v1/vault/keys2/{id}/archive
Archive - post

/v1/vault/keys2/{id}/recover
Recover - post

/v1/vault/keys2/{id}/revoke
Revoke - post

/v1/vault/keys2/{id}/export
Export - post

/v1/vault/keys2/{id}/clone
Clone - post

/v1/vault/query-keys/
Query - post

Users

/v1/usermgmt/users/
List - get
Create - post

/v1/usermgmt/users/{user_id}
Get - get
Delete - delete
Update - patch

/v1/auth/self/user
Get - get
Update - patch

/v1/auth/changepw
Change password - patch

/v1/usermgmt/pwdpolicies/global
Change password policy - patch
Get password policy - get

REST API

The REST API is hosted at this base URL: `https://{addr}/api/v1` You can use the REST interface via **curl**, or from the "API playground".

To copy and paste the following example commands, set an environment variable to point to your CipherTrust Manager instance:

```
$ export KSCTL_URL=https://{addr}              # sh/bash
$ set -x KSCTL_URL=https://{addr}              # fish
```

For example, this command will use the root admin's credentials to create an API token:

```
$ curl -k -X POST $KSCTL_URL/api/v1/auth/tokens/ \
    -H "Content-Type: application/json" \
    -d "{\"name\":\"admin\",\"password\":\"admin\"}"
```

/v1/audit/alarm-configs/{id}
Get - get
Update - patch
Delete - delete

/v1/audit/client-records
List - get

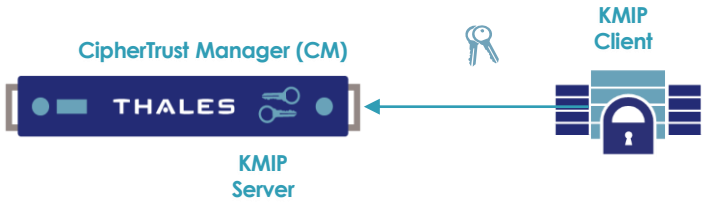
/v1/audit/client-records/{id}
Get - get

THALES

Thales KMIP właciwości

KMIP is an industry-standard protocol for encryption key exchange between clients (appliances, storages) and a KMS servers (CM).

- Separating keys from the encrypted data
- Allow utilize a corporate policies
- Supported key types - Symmetric Key, Public Key, Private Key, Secret Data, Opaque
- Supported Operations – Activate, Delete Attribute, Get Attributes List, Register, Add Attribute, Destroy, Locate, Re-key, Check, Discover Versions, MAC, Re-key Key Pair, Create, Encrypt, MACV, Revoke, Create Key Pair, Get, Modify Attribute, Decrypt, Get Attributes, Query (based on KMIP 1.0-1.4)
- All clients has to be registered and approved for KMIP connection



THALES

Rozwiązanie – dostępność

$$A = \frac{MTBF}{MTBF+MTTR} * 100\%$$

MTBF=**165297 h**
MTTR = (next business day + weekend + delivery in EU) =>
1+2+2 => **5 dni** (120h)

A = 165 279 / (165 279 + 120) *100% = **99,92 %**

MTTR = (20 business days to repair) => **20 dni** (480h)

A = 165 279 / (165 279 + 480) *100% = **99,71%**

Ax dostępność poj. węzła

n - ilość węzłów

$$A = (1 - (1 - Ax)^n) * 100\%$$

A = (1 – (1-0.9992) ^2) *100% = **99,999936%**

A = (1 – (1-0.9971) ^2) *100% = **99,999159%**

Technical Support SLAS

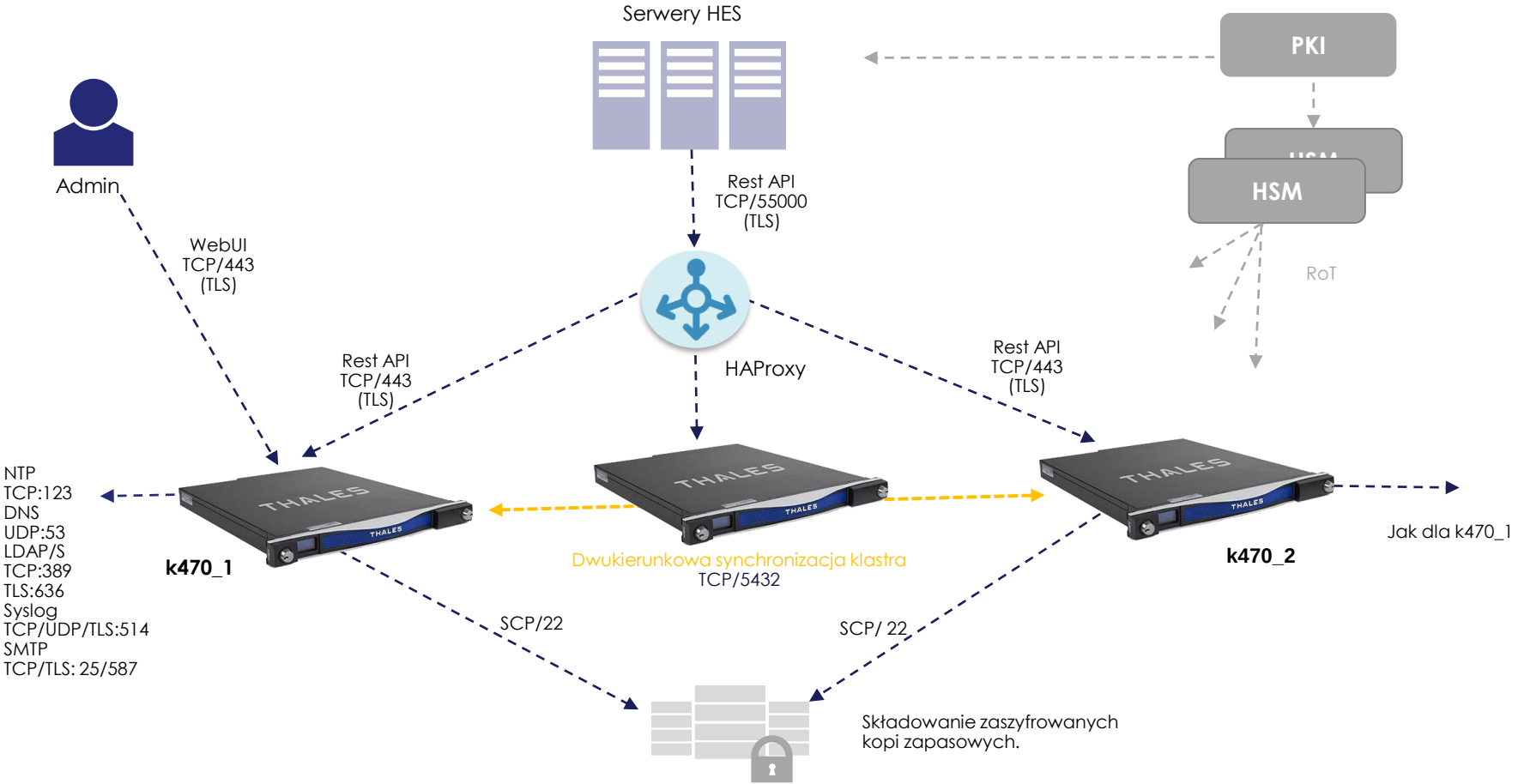
Support Offerings	Premier	Enhanced	Standard	Original Warranty
Hours of coverage	24 x 7 x 365 coverage	24 x 7 x 365 coverage	8 x 5 regional business hours only*	8 x 5 regional business hours only*
1st Response Target	✓ 30 Minutes for Critical issues ✓ 4 Hours for high issues	✓ 1 Hour for Critical issues ✓ 4 Hours for high issues	8 Business Hours	24 Hours
Web / Portal Access	Portal and Phone Support	Portal and Phone Support	Portal and Phone Support	Portal Support Only
Additional Support Options	✓ Account Reporting and Management ✓ 2 Certification Credits ✓ Option to purchase a Named Engineer	✓ 1 Hour for Critical issues ✓ 4 Hours for high issues	8 Business Hours	24 Hours
Equipment Replacement ****	Next Business Day advanced shipment after RMA and service entitlement verification***	Next Business Day advanced shipment after RMA and service entitlement verification***	20-business-day replacement (Receipt to Shipment)**	20-business-day replacement (Receipt to Shipment)**
Firmware, Minor Updates, and Patches	All updates available at no charge	All updates available at no charge	All updates available at no charge	Not available
Updates for standalone software	All updates available at no charge	All updates available at no charge	✓ No charge for minor releases ✓ Discounts toward major releases	No available

Table 1-Downtime of availability

Availability	9s	Downtime
90%	One	36.5 days/year
99%	Two	3.65 days/year
99,9%	Three	8.76 hours/year
99,99%	Four	52 minutes/year
99,999%	Five	5 minutes/year
99,9999%	Six	31 seconds/year

THALES

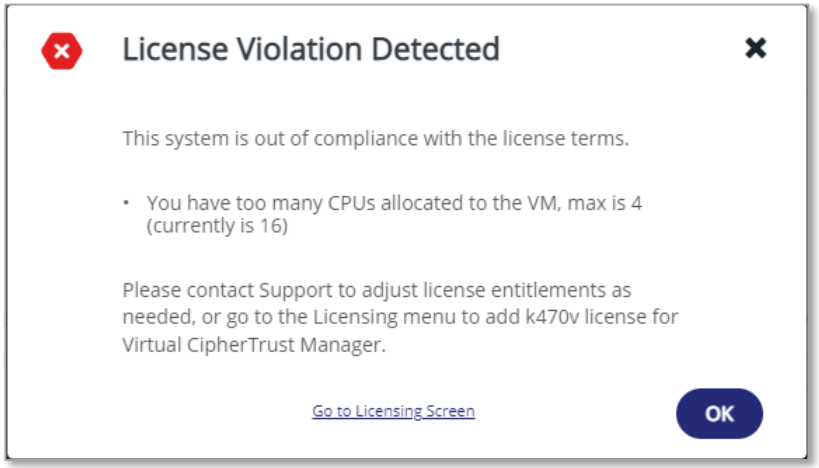
Architektura rozwiązania



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

- **Korzystanie z Rest API nie wymaga żadnej licencji na konektory! W odróżnieniu od np. KMIP**

- **Przetestowanie wirtualnej wersji k470v wymaga licencji. Wszystkie wersje trial czy Cummnity Edition to wersje „k170v”**



Anyhow, we do not limit the CPUs on CM technically. It means all 16 CPUs on your CM would work

THALES

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

CM (k170v na vSphere 7.x):

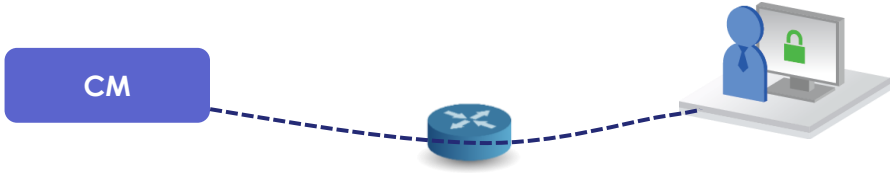
- Pojedyncza instancja
- 2 CPU
- 16 GB RAM
- 60 GB HDD
- 1x NIC (1Gbps)

Klient:

- DELL Latitude 5521, i7 2,5GHz, 32GB RAM, W10 Ent. 20H2

Wywołania RestAPI (Python 3.1)

- Uwierzytelnienie user/pwd




```
Administrator: C:\WINDOWS\system32\cmd.exe

C:\Python310>ping 10.10.11.233

Pinging 10.10.11.233 with 32 bytes of data:
Reply from 10.10.11.233: bytes=32 time=35ms TTL=63
Reply from 10.10.11.233: bytes=32 time=5ms TTL=63
Reply from 10.10.11.233: bytes=32 time=6ms TTL=63
Reply from 10.10.11.233: bytes=32 time=5ms TTL=63

Ping statistics for 10.10.11.233:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 35ms, Average = 12ms

C:\Python310>
```

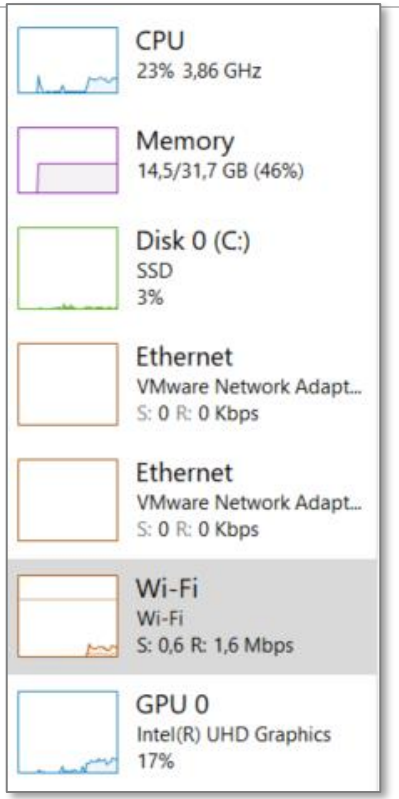

THALES

Wyniki test1

CMKexportMulti2.py

- ciphertrust_manager = '10.10.11.233'
- **tts = 10** # number of threads to start (try: 1..20)
- **mkte = 50** # maximum attempts to export a key by thread (1..50).

10 x 1,66 = 16,6 kluczy /s




```
0 Average # of keys exported by thread per second:  1.6119491486197173
1 Average # of keys exported by thread per second:  1.661647644860848
2 Average # of keys exported by thread per second:  1.755365150046518
3 Average # of keys exported by thread per second:  1.6970259764448665
4 Average # of keys exported by thread per second:  1.6978314491468818
5 Average # of keys exported by thread per second:  1.654886104662626
6 Average # of keys exported by thread per second:  1.607904458908828
7 Average # of keys exported by thread per second:  1.6943287872597261
8 Average # of keys exported by thread per second:  1.5535653318065394
9 Average # of keys exported by thread per second:  1.62185971709083
```

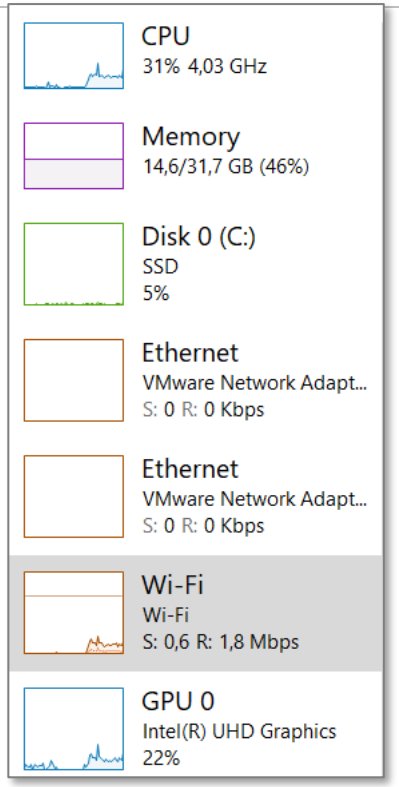
Wyniki test2

CMKexportMulti2.py

- ciphertrust_manager = '10.10.11.233'
- **tts = 20** # number of threads to start (try: 1..20)
- **mkte = 50** # maximum attempts to export a key by thread (1..50).

20 x 1,32 = 26,4 kluczy /s

```
0 Average # of keys exported by thread per second:  1.2875863307192805
2 Average # of keys exported by thread per second:  1.3873089942308798
1 Average # of keys exported by thread per second:  1.276728111475794
3 Average # of keys exported by thread per second:  1.3525560114312818
4 Average # of keys exported by thread per second:  1.3257499274967866
5 Average # of keys exported by thread per second:  1.3070069973403993
...
14 Average # of keys exported by thread per second:  1.2630951246351443
15 Average # of keys exported by thread per second:  1.3027576753639432
16 Average # of keys exported by thread per second:  1.3129874719208052
18 Average # of keys exported by thread per second:  1.4079678369065967
19 Average # of keys exported by thread per second:  1.4109129781338938
17 Average # of keys exported by thread per second:  1.2250696247093342
```

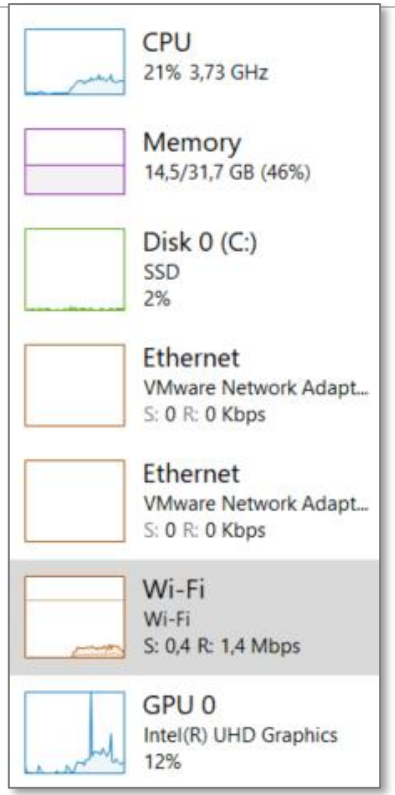


Wyniki test3

CMKexportMulti2.py

- ciphertrust_manager = '10.10.11.233'
- **tts = 20** # number of threads to start (try: 1..20)
- **mkte = 100** # maximum attempts to export a key by thread (1..50).

20 x 1,31 = 26,2 kluczy /s

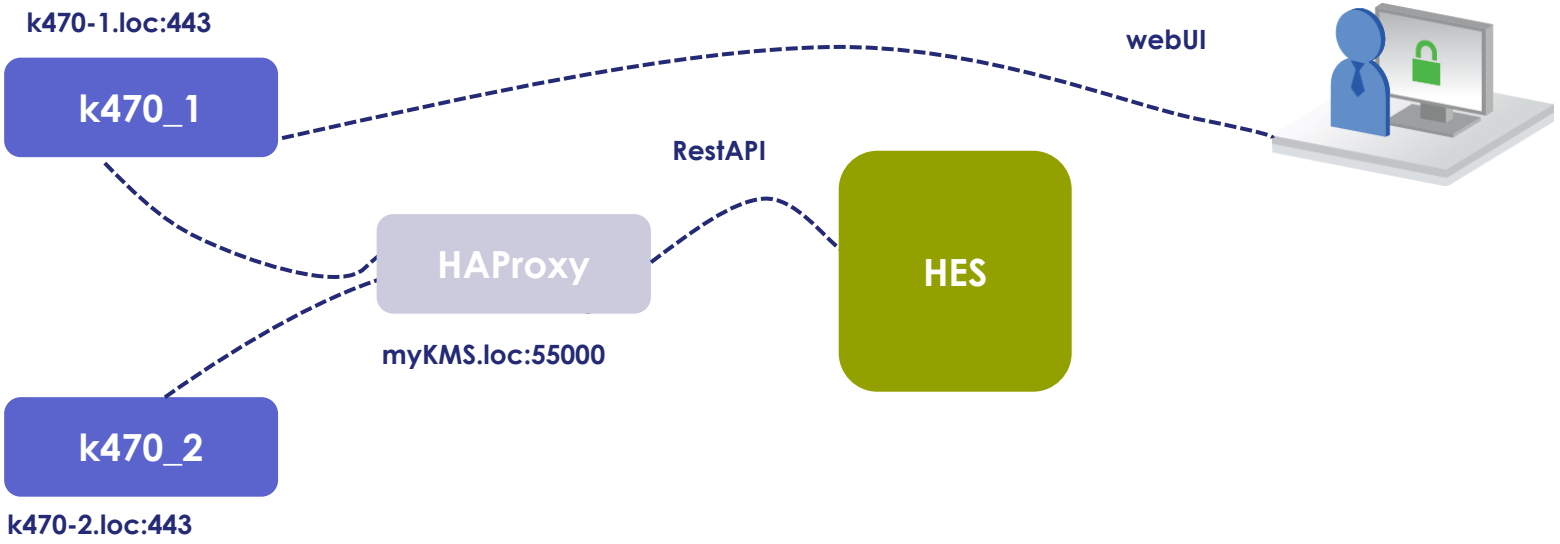



```
0 Average # of keys exported by thread per second:  1.2879982689308545
1 Average # of keys exported by thread per second:  1.2956935575537483
2 Average # of keys exported by thread per second:  1.3517273309172986
3 Average # of keys exported by thread per second:  1.349582222825186
4 Average # of keys exported by thread per second:  1.3663033954012616
...
14 Average # of keys exported by thread per second:  1.3081842285749627
15 Average # of keys exported by thread per second:  1.2992724744179156
18 Average # of keys exported by thread per second:  1.3862494790582118
16 Average # of keys exported by thread per second:  1.273860266130085
17 Average # of keys exported by thread per second:  1.2776877548073509
19 Average # of keys exported by thread per second:  1.3301340673838877
```

Tego raczej nie znajdziecie w dokumentacji.

Czy współpracujemy z HAProxy?

- TAK! I to bardzo dobrze, wystarczy prosta konfiguracja (round-robin)
- Jedna uwaga: ruch do konsoli zarządzającej nie kierujemy przez HA Proxy dla uniknięcia „ogłupienia przeglądarki"

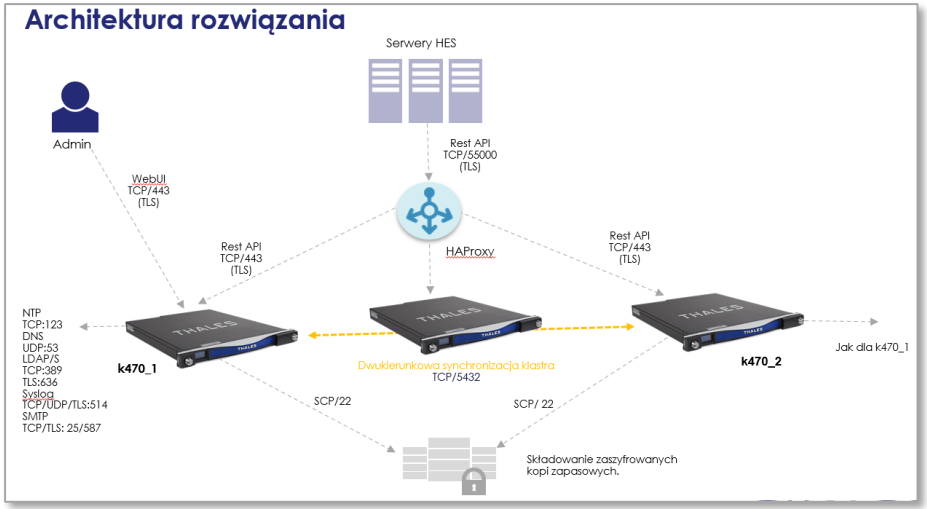


CryptoPanel

podsumowanie

Podsumowanie i słowo o tym co do wyceny

- **CM jako „serce” rozwiązania**



- **produkty dostępne w kanale partnerskim**
- **rozwiązania demo?: tak urz. wirtualne**
- **zalecane zastosowanie HSM jako RoT**

Wycena:

- **3x CipherTrust Manager Appliance k470 (40 000 € netto / urz.)**
- **3x Enhanced Support (18%)**
- **Opcja: urządzenie zapasowe (dla b. krótkich czasów reakcji)**

CryptoPanel

CryptoPanel

TEST WIEDZY #18

Centralne repozytorium oraz zarządzanie poświadczeniami i kluczami szyfrującymi dla rozwiązań OT i IoT

CryptoPanel #18 – bądź pierwszy, odbierz zestaw plażowy!

- Zapraszamy do testu wiedzy z tematu: *„Centralne repozytorium oraz zarządzanie poświadczeniami i kluczami szyfrującymi dla rozwiązań OT i IoT.”*
- Uwaga: **5 najszybszych i poprawnych** odpowiedzi nagradzamy zestawem plażowym Thales!

- Przy wypełnianiu formularza prosimy podać (aby móc zidentyfikować uczestnika!):
  - **Imię i Nazwisko**
  - **Adres e-mail**

Link do quiz... (będzie także w czacie)

https://forms.office.com/e/KBi59Xa3cK

https://tinyurl.com/y77bmdvn

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/
- REST API: https://thalesdocs.com/ctp/cm/2.11/admin/cm_admin/rest-api/index.html