

# CyberSecurityPanel

edycja #31

Już za moment  
zaczynamy...



# CyberSecurityPanel

edycja #31



**THALES**  
Building a future we can all trust

**CLICO**

# CyberSecurityPanel

17 LUTEGO 11:00

**Budowa ultra wysokodostępnych  
środowisk zarządzania kluczami  
szyfrującymi (KMS) dla  
infrastruktur w zasobach lokalnych  
i chmurowych**

Dyskusje poprowadzą: Piotr Majek i Jarosław Ulczok

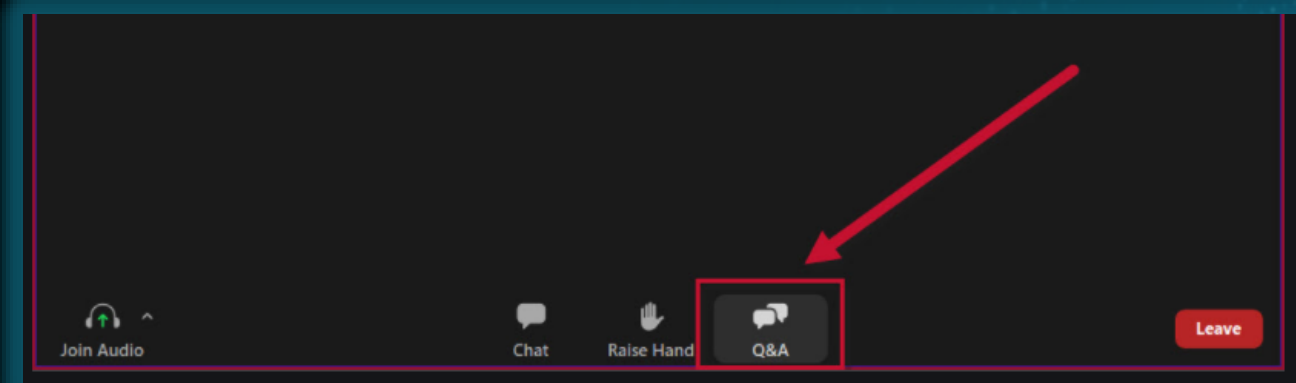
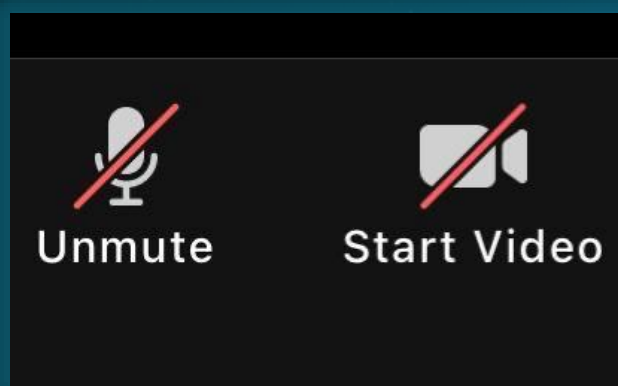
**THALES**  
Building a future we can all trust

**CLICO**



# CyberSecurityPanel

edycja #31



# CyberSecurityPanel

problem



# Nasze wyzwanie (czyli co i jak chcemy osiągnąć)

- Poszukujemy rozwiązania zarządzania kluczami szyfrującymi (KMS) umożliwiającego stworzenie klastra w trybie „ultra” wysokiej dostępności w celu obsługi integracji:
  - KMIP
  - Zarządzania kluczami w chmurze Azure (KeyVault)
  - i innych w przyszłości (RestAPI)
- Obecnie korzystamy z rozwiązania KMS(K470) + HSM (Luna7)
- KMS ma obsługiwać systemy wdrożone zarówno on-prem, jak i w chmurze
- Automatyzacja czynności operacyjnych (np. monitorowanie, aktualizacje)
- HSM jako RoT dla każdej instancji KMS (wymóg bezpieczeństwa)
- Wybrać HW czy VM? Co będzie lepsze?
- Czy można przeprowadzić rozszerzenie w locie?
- Chcemy zachować operacyjność przy awarii (całkowitej) 2 z 3 ośrodków.
- Wysoka dostępność musi być zapewniona także wewnątrz poszczególnych ośrodków obliczeniowych.
- Jeden z DC musi być „chmurowy”.

# CyberSecurityPanel

rozwiązanie

**THALES**  
Building a future we can all trust



**Zaczynamy od...**

# Architektura (dziś)

Dwa ośrodki przetwarzania danych

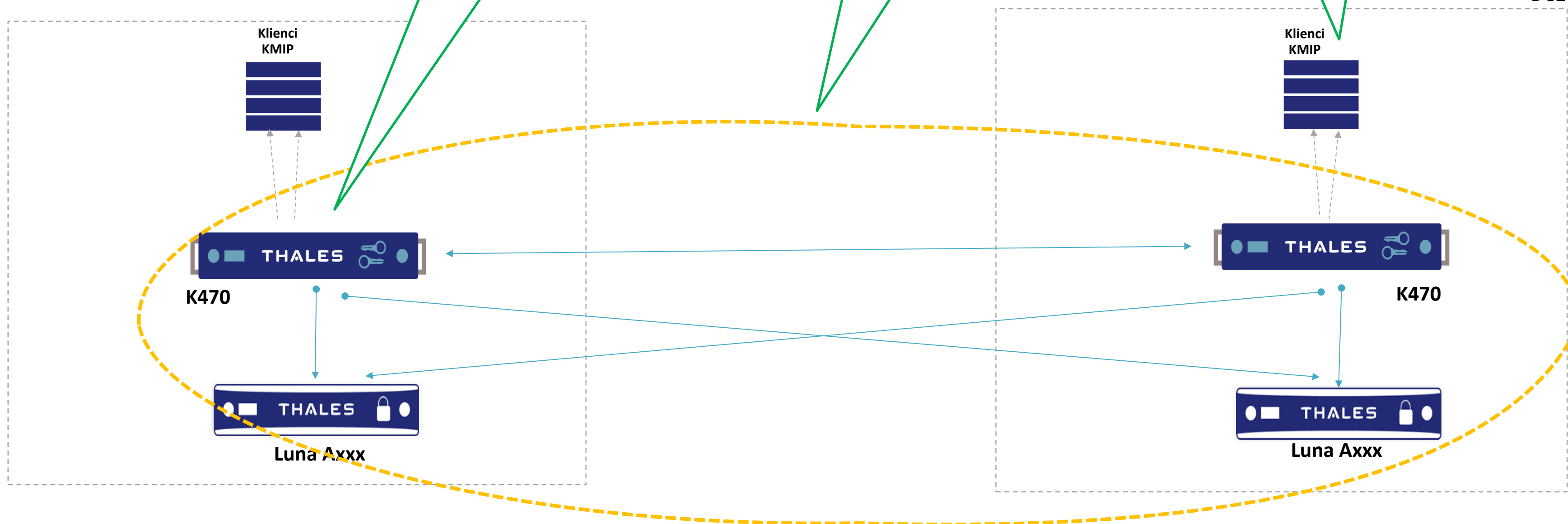
Klaster KMS zbudowany w oparciu o urządzenia K470

Klaster logiczny KMS rozciągnięty geograficznie

Integracja z rozwiązaniami firm 3. z wykorzystaniem KMIP

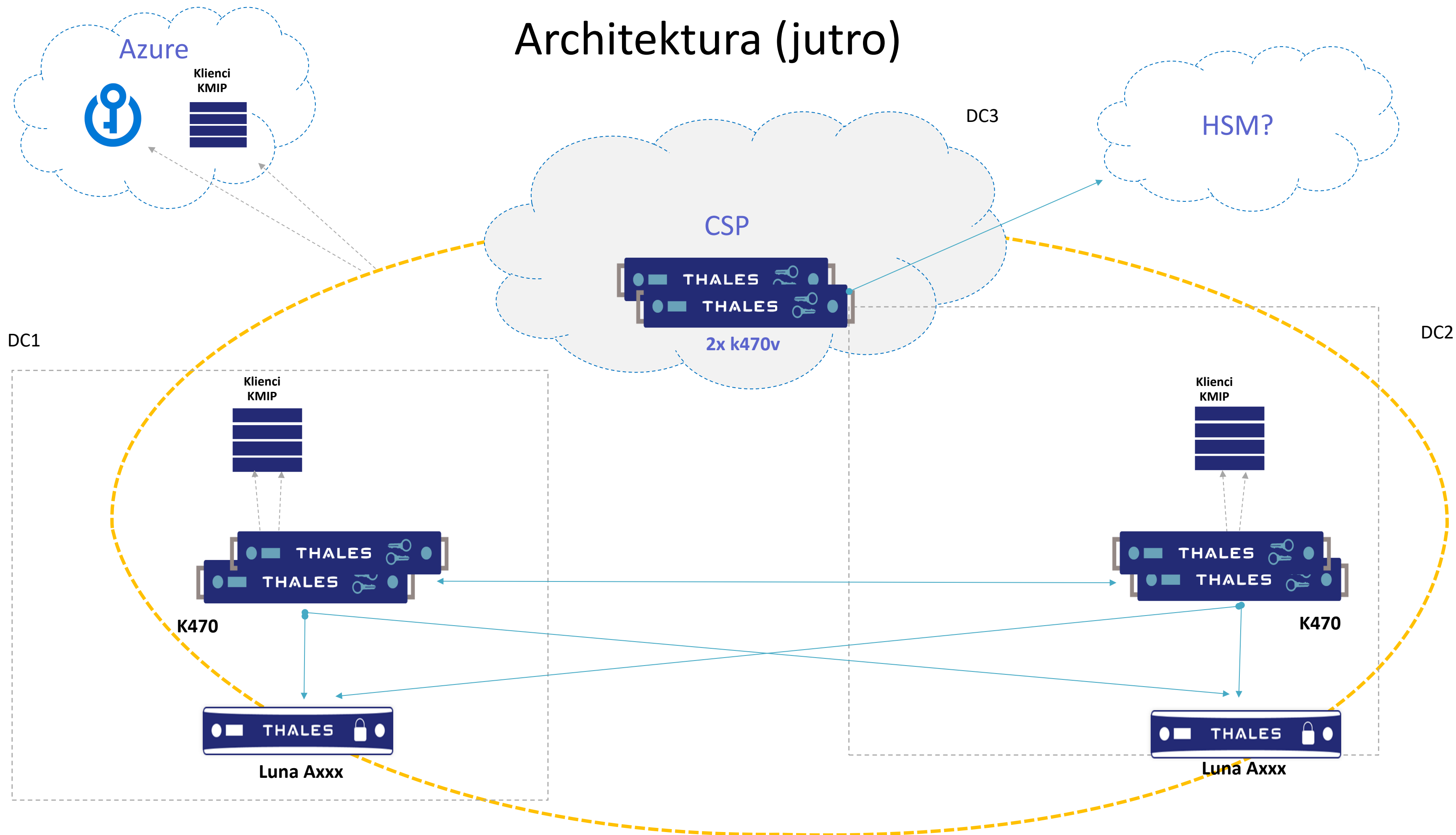
DC1

DC2



**Doprowadźmy do...**

# Architektura (jutro)



# Rozwiązanie

rozwiązanie (język polski)

[ edytuj ]

wymowa:

IPA: [ˌrɔzvʲɔɫ̪ˈzãɲɛ], AS: [rɔzvˈɫɔʝzãɲɛ], zjawiska fonetyczne: *zmiękk. • nazal. • asynch. ą • -ni...* • *akc. pob. • i → j* 

znaczenia:

*rzeczownik, rodzaj nijaki*

(1.1) załatwienie czegoś, poradzenie sobie z czymś; wynik, rezultat jakiegoś działania

(1.2) konsekwencja, wynik poszukiwań

(1.3) zaprojektowanie lub zrealizowanie planów architektonicznych, artystycznych

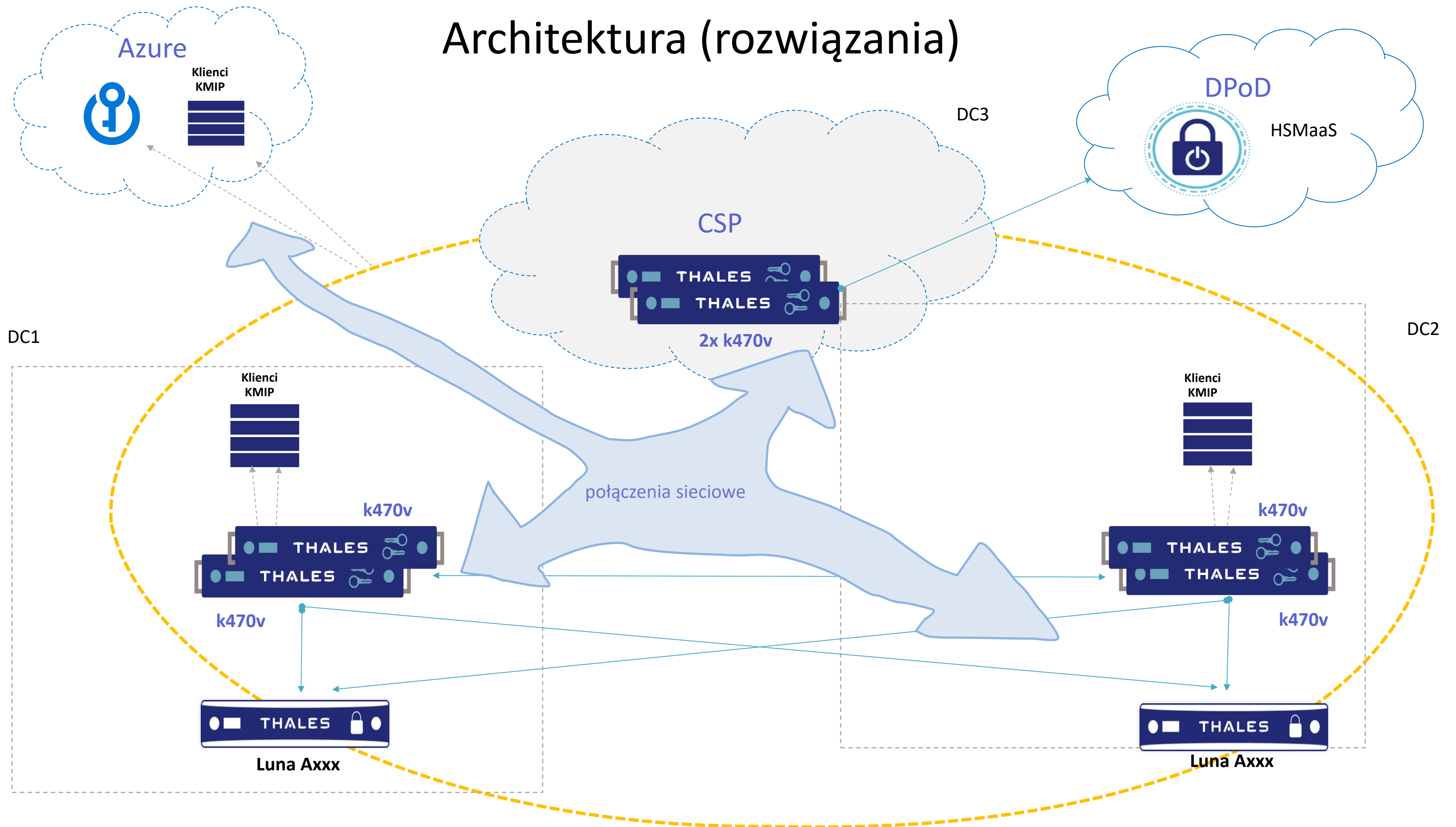
(1.4) poród, przyjście dziecka na świat

(1.5) *mat. wynik*

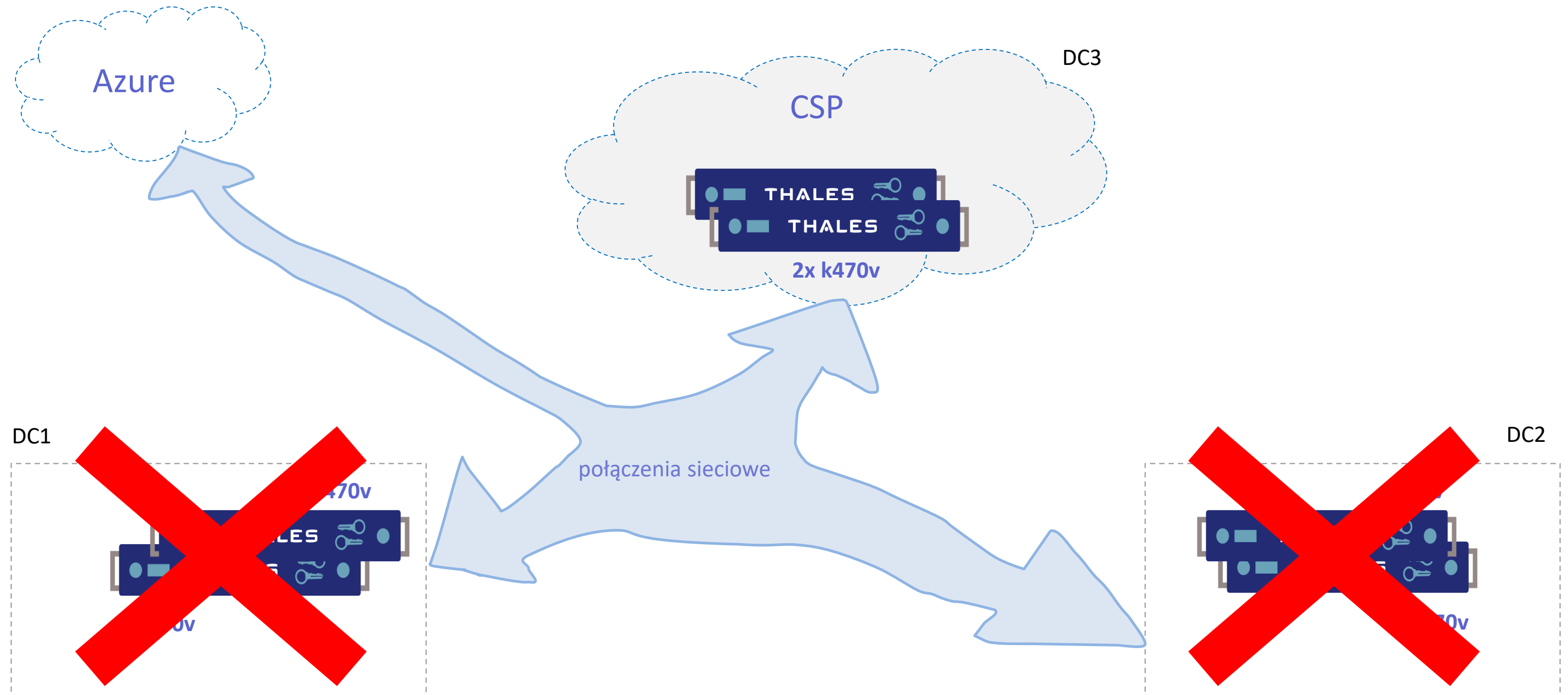
(1.6) przerwanie jakiejś działalności; rezygnacja z tworzonego wcześniej związku (lub relacji, grupy)

(1.7) *rzecz. odczas. od* rozwiązać

# Architektura (rozwiązania)



# Wysoka dostępność (rozwiązania)

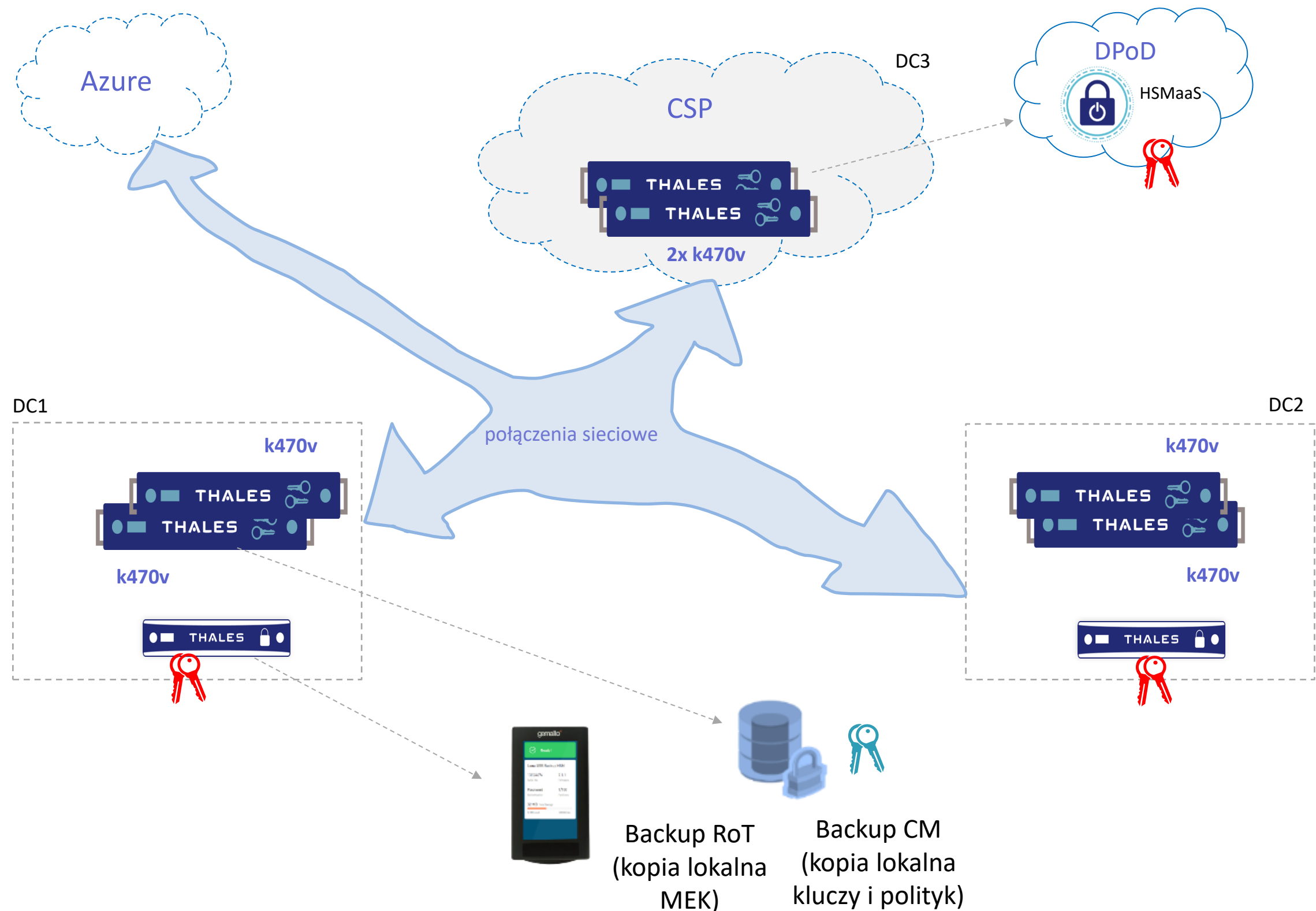


**Jak to zbudować?**

# Kroki do zbudowania rozwiązania

Założenie: działający klaster w oparciu o 2x K470+Luna A7xx (jako RoT)

1. **Aktualizujemy** K470 do najnowszej wersji
2. Wykonujemy **backup systemowy** K470 (zawiera wszystkie klucze)
3. Wykonujemy **backup kluczy z partycji RoT** na Luna A7xx
4. Wdrażamy dostęp do partycji HSMaaS w DPoD i **odtworzymy** tam **materiał zbackupowany z partycji RoT**
5. Instalujemy 2x k470v w DC3 z RoT w oparciu o partycję w DPoD.
6. **Dołączamy** instancje k470v w DC3 do istniejącego klastra K470 (jedna po drugiej).
7. **Instalujemy** instancje k470v w DC1 i DC2, integrujemy z RoT (tu Luna A7xx) i **dołączamy** obie do istniejącego klastra.
8. **Usuwamy** instancje K470 w DC1 i DC2 z klastra.
9. **Instalujemy** drugie instancje k470v w DC1 i DC2, integrujemy z RoT (tu Luna A7xx) i **dołączamy** obie do istniejącego klastra.
10. Wykonujemy backup systemowy k470v
11. Gotowe



# CyberSecurityPanel

podsumowanie



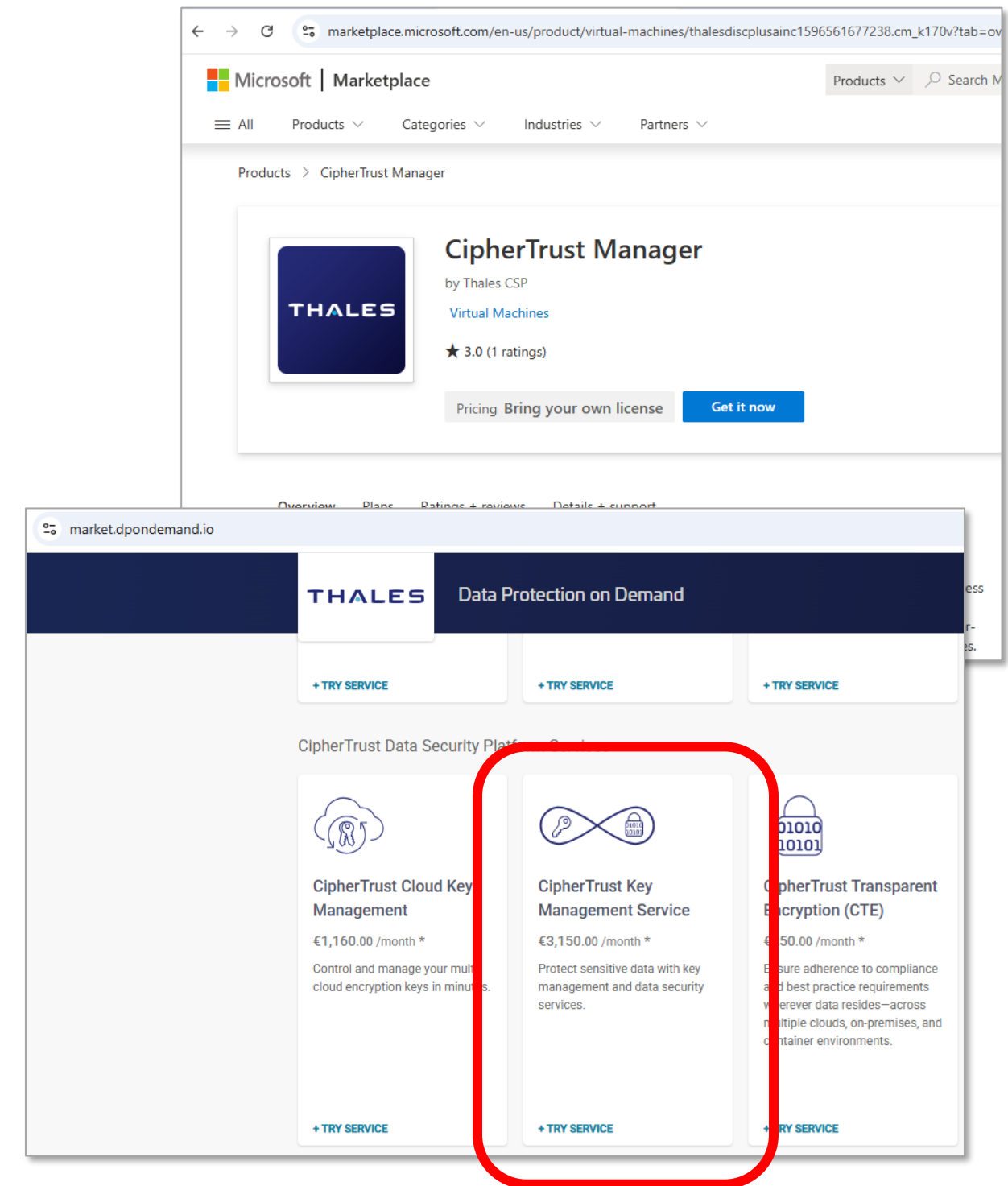
# Coś na wynos

- CM pozwala na elastyczne budowanie **wysokodostępnych klastrów logicznych** rozwiązań Key Management System
  - W wielu przypadkach zewnętrzne równoważenie obciążenia do klastra nie jest konieczne (w zależności od protokołu lub dostępu)
- W klastrze można „mieszać” urządzenia fizyczne (**K470**) i wirtualne CM (**k470v**)
  - Choć nie zalecamy tego!
  - Koniecznie ta sama wersja oprogramowania na wszystkich węzłach klastra.
- **Różnice** pomiędzy K470 a k470v?
  - Większa elastyczność (wydajność, pojemność) z k470v
  - Brak inwestycji w platformę w przypadku k470
  - [https://cpl.thalesgroup.com/sites/default/files/content/product\\_briefs/ciphertrust-manager-pb.pdf](https://cpl.thalesgroup.com/sites/default/files/content/product_briefs/ciphertrust-manager-pb.pdf)

| 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, Google Cloud 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, Google Cloud 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, Google Cloud HSM | <b>Built-in HSM</b> , 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, Google Cloud 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 140-2 L1 (Certificate #4430) |                                                                                                                                                                                                          |                                                                                                                                                                                                          |                                                                                                                                                                                                          |                                                                                                                                                                                                                                |

# Coś na wynos cd.

- Wygodna aktualizacja (upgrade) klastra CM.
  - On-line In-place
  - Cluster Remove/Rebuild
- CipherTrust Manager jest dostępny w większości CSP
  - Możliwa automatyzacja (np. TerraForm) wdrożenia i konfiguracji
  - BYOL / oferta Clico
- Ponadto: CipherTrust Manager jest także dostępny jako usługa SaaS (CMaaS),
  - ale nie można łączyć jej w klastry z CM wdrożonym lokalnie (on-prem/cloud)
  - <https://market.dpondemand.io/>
- CM do Q3 2026 będzie całkowicie „PQC Proof”
  - Zarówno w zakresie komunikacji zewnętrznej jak i komponentów wewnętrznych (certyfikaty, podpis kodu)



**Nauczki...**

Tego raczej nie znajdziecie... no chyba, że w dokumentacji 😊 1/2

## Klaster CipherTrust Managera – podstawowe własności, warto wiedzieć!

- The **maximum** number of cluster **nodes is 20**. Joining a 21st node will fail.
  - Rekomendujemy 4-6 węzłów w klastrze
- Nodes in a cluster communicate over port 5432. Members of the cluster must have **bi-directional** access to each other on port **5432/TCP (TLS)**.
- For proper cluster functionality, every node must be synchronized to **the same time**. Otherwise, communication between nodes fails.
  - Manually configure the same NTP server for each node.
  - The NTP server configuration is not replicated, so you must configure each node independently
- Good **connectivity** is required **between every node**. Because each node is continuously connected to every other node, network issues can cause synchronization problems across nodes, creating maintenance and troubleshooting overhead.
  - **stabilna sieć o niskim opóźnieniu**
  - z praktyki (ale nie łapcie nas za słowa 😊) : <100 ms

Tego raczej nie znajdziecie... no chyba, że w dokumentacji 😊 2/2

## Klaster CipherTrust Managera – co **nie jest** synchronizowane w klastrze?

Most things (*klucze, polityki, użytkownicy, ...*) replicate across the cluster.

However, the following items are specific to an individual node, and **are not clustered**

- Backup files
- Backup keys
- Debug, KMIP Activity, and NAE Activity **logs**
- NTP configuration
- **HSM configuration**
- Instance name
- Virtual CipherTrust Manager **license**
- Interface certificates
- Proxy settings

# CyberSecurityPanel

pytania i odpowiedzi



# CyberSecurityPanel

