CryptoPanel

edycja #9

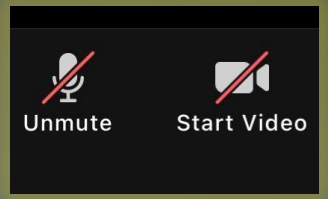
za chwilę zaczynamy...

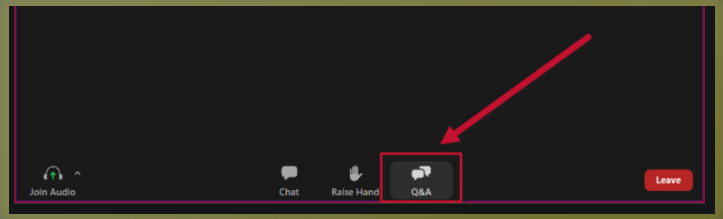
CryptoPanel

THALES

CLICO

CryptoPanel





CryptoPanel

edycja #9

Konteneryzacja zmienia podejście do architektury aplikacji i infrastruktury. Czy i ewentualnie jak można chronić dane poprzez szyfrowanie w środowisku Docker i Kubernetes?

CryptoPanel

dziś dyskutują

Piotr Wróbel

Regional Sales Manager
Piotr.Wrobel@thalesgroup.com
mob. +48 669 88 99 76

Jarosław Ulczok

Pre-sales Consultant
Jaroslaw.Ulczok@thalesgroup.com
mob. +48 603 056 667

CryptoPanel

problem

co nas boli...

- Jesteśmy ubezpieczycielem
- Posiadamy aplikację webową – portal klienta
- System przetwarza dane osobowe klientów
- Zlokalizowany jest w naszym centrum przetwarzania
- Jest jednym z kluczowych systemów z punktu widzenia biznesowego – klient ma wgląd w aktualne polisy, może kupić nowe produkty, zmienić dane itp.

- ...że aplikacja webowa ma nieco archaiczny wygląd
- ...że niezbyt dobrze pracuje w środowisku urządzeń mobilnych
- ...modyfikacja, rozszerzenie funkcjonalności wymaga zbyt dużych nakładów pracy, przy jednoczesnym pozostaniu przy starej architekturze
- ...że rozwój aplikacji w obecnej architekturze powoduje zbyt daleko idące kompromisy związane m.in. z brakiem np. należytej ochrony przetwarzanych informacji, brak skalowalności
- ...że nie mamy wiedzy jak podejść do tematu bezpieczeństwa danych jeśli zostanie wybrany scenariusz budowy nowej aplikacji w oparciu o mikroserwisy oraz dodatkowo potencjalne wykorzystanie środowiska chmurowego

CryptoPanel

rozwiązanie

Na początek ...
... co to są kontenery?
K8s – czyli WTF?

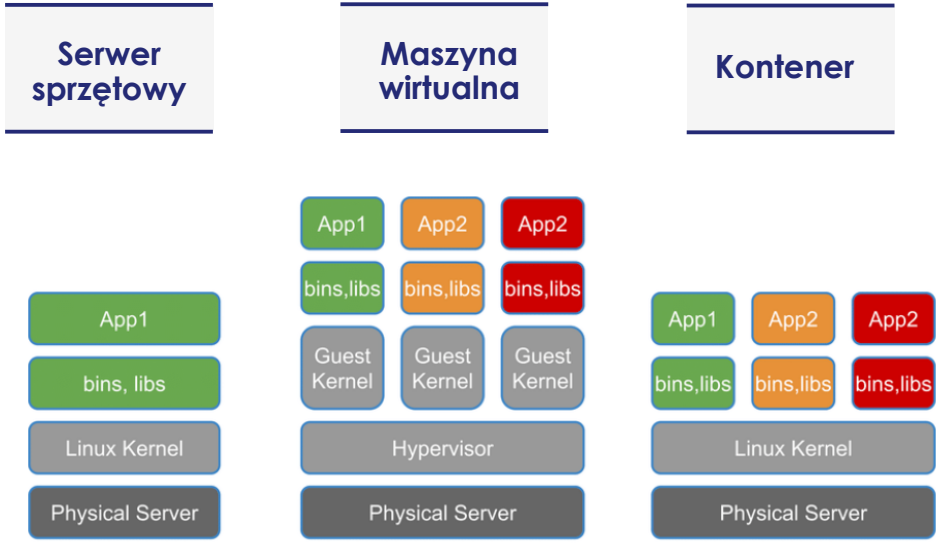
Gdzie działają aplikacje?

Kolejne ważne miejsce po maszynach wirtualnych dla twórców aplikacji

Kontenery

Zalety korzystania z technologii konteneryzacji

- Kontenery są izolowane od siebie
- Aplikacje mają wszystko, czego potrzebują
- Kontenery są znacznie bardziej elastyczne niż maszyny wirtualne
- Zwiększają zwinność i skracają czas wprowadzenie na rynek (TTM)
- Zapewniają „lepszy" rozwój aplikacji



THALES

Lepsz tworzenie aplikacji

Powstaje Serwis Ubezpieczeniowy…

Aplikacja monolityczna

Strona ubezpieczyciela

- Klient
- Polisy
- Agenci

Zastosowanie mikroserwisów

Strona ubezpieczyciela

Klient

Polisy

Agenci

Kontenery (Docker)

Tworzymy kontenery dla swoich aplikacji

?

THALES

Lepsz tworzenie aplikacji

Powstaje Serwis Ubezpieczeniowy…

Aplikacja monolityczna

Strona ubezpieczyciela

- Klient
- Polisy
- Agenci

Zastosowanie mikroserwisów

Strona ubezpieczyciela

Klient

Polisy

Agenci

Kontenery (Docker)

Tworzymy kontenery dla swoich aplikacji

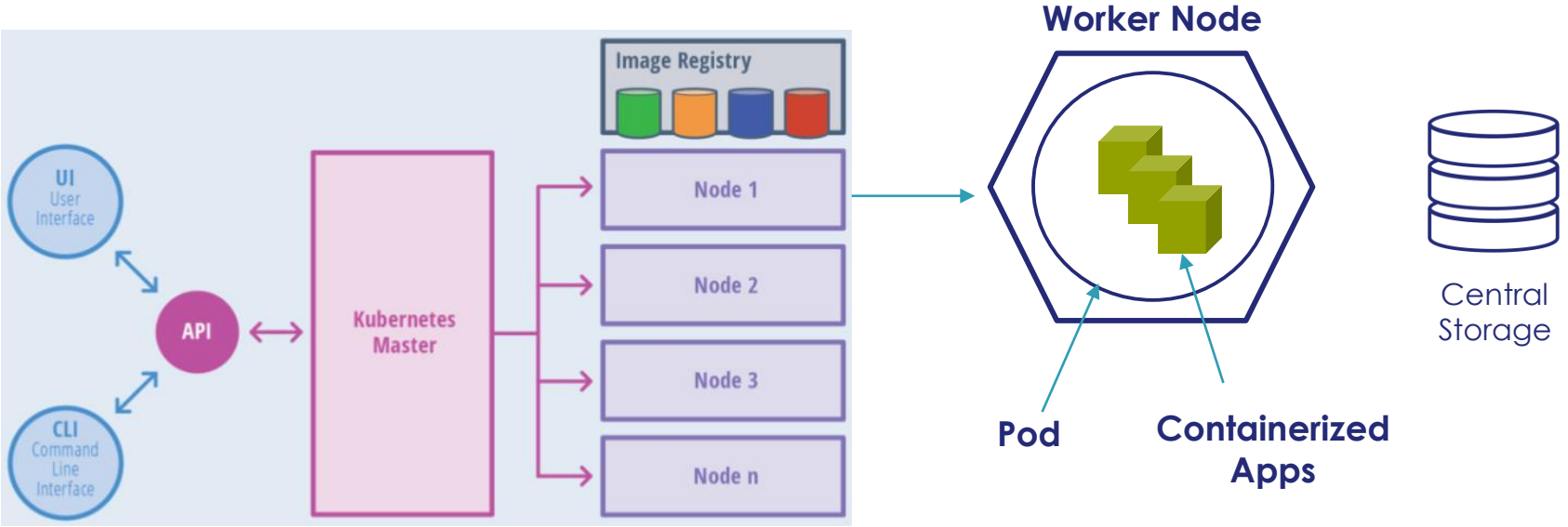
Kubernetes

Uruchom i aranżuj swoje aplikacje w kontenerach z Kubernetes

THALES

Kubernetes

Architektura



THALES

Po co mi ten Kubernetes?

- Przecież można ręcznie zarządzać kontenerami za pomocą np. platformy Docker?
- Generalnie, nie polecamy…

*Netflix says it uses the platform, which launches **as many as three million containers per week**, to host thousands of applications over seven regionally isolated stacks across tens of thousands of EC2 virtual machines.*[20 kwi 2018]

https://www.datacenterknowledge.com/cloud/netflixs-container-management-system-now-open-source

Technologia kontenerów w różnych smakach

Może być dostarczona na różne sposoby

On Premise	Google	AWS	Azure
Docker OpenShift Kubernetes	Google Kubernetes Engine Cloud Run Google Compute Engine	Elastic Container Services Elastic Kubernetes Services AWS Fargate EC2 AWS App Runner Amazon ECS Anywhere EKS Anywhere ROSA	Azure Kubernetes Service Azure Red Hat OpenShift Azure Container Apps Azure Functions Web-App for Container Container Instances Service Fabric Container Registry

I wiele innych…

THALES

Aspekty bezpieczeństwa w kontekście konteneryzacji jakie powinniśmy uwzględnić

Co uwzględnić przy tworzeniu aplikacji za pomocą kontenerów?

1. Zarządzanie dostępem

- Unikaj uruchamiania kontenerów w trybie uprzywilejowanym (root).
- Obierz wszystkie domyślne uprawnienia a następnie dodaj niezbędne.
- Ogranicz dostępne zasoby (RAM, CPU).

2. Bezpieczeństwo obrazów

- Używaj oficjalnych, popularnych i minimalistycznych obrazów.
- Wymagaj od obrazów podpisu cyfrowego.

3. Zarządzanie sekretami

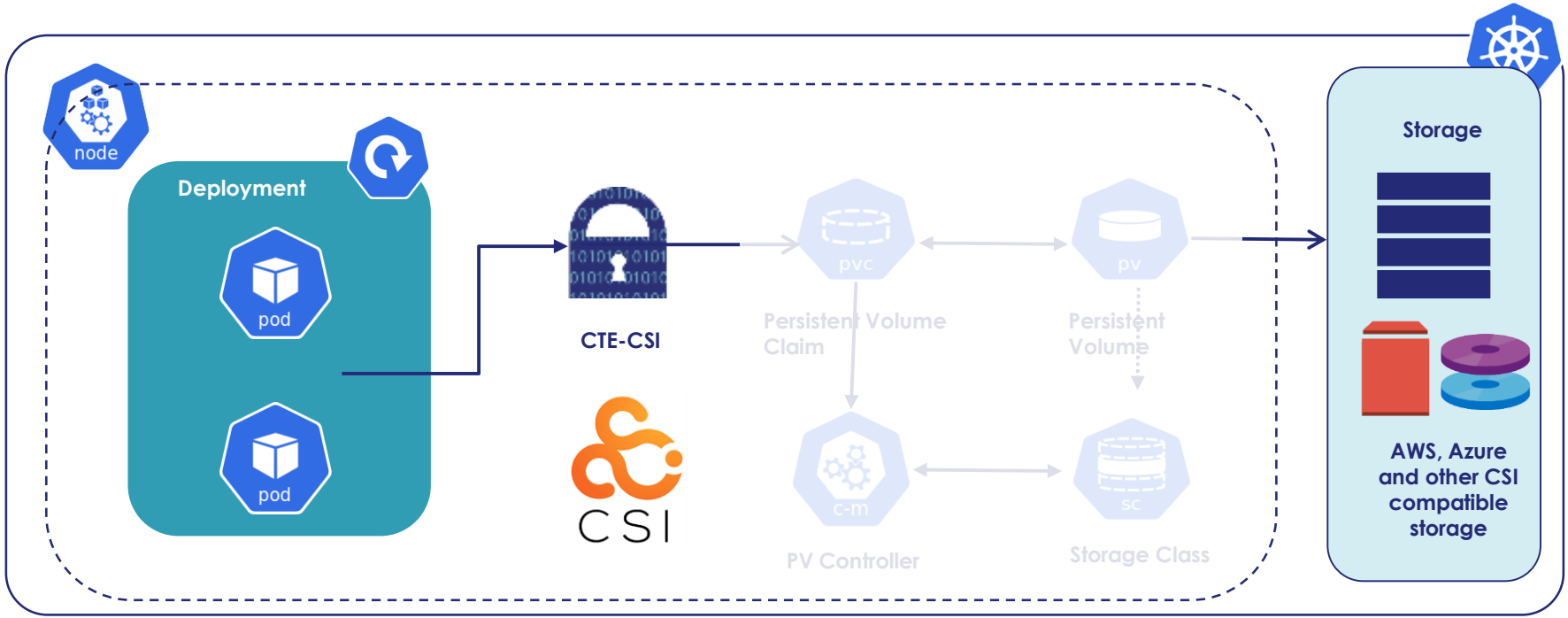
- Używaj sekretów lub wolumenów.
- Rozważ używanie sejfów.

4. Przechowuj **wrażliwe dane w wolumenach**, nigdy w kontenerach

Rozwiązanie…

Schemat działania: CTE Container Storage Interface

*CTE CSI** umożliwia skonteneryzowanej aplikacji interakcję z istniejącą, trwałą pamięcią masową, zapewniając transparentną ochronę danych.

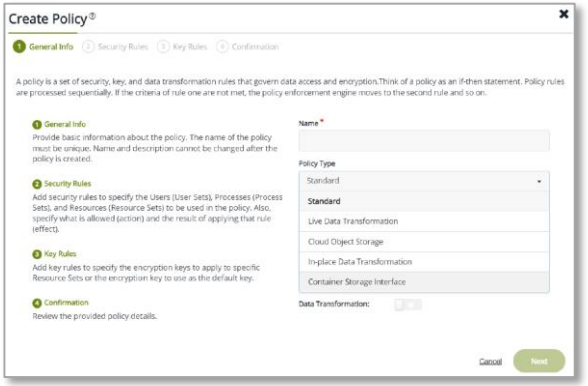


THALES

CipherTrust Transparent Encryption z CSI

CTE kontroluje szczegółowo zabezpieczenia Pod-ów Kubernetes

- CTE-CSI jest dla Kubernetes – Docker to za mało!
- CTE-CSI dla K8s jest zarządzane przez CipherTrust Manager



Szyfrowanie, kontrola dostępu i bezpieczeństwa per kontener

- Szyfruj dane generowane i przechowywane na trwałym woluminie dołączonym do aplikacji kontenerowej
- **Możliwość wdrożenia dla przypadków użycia *Kubernetes as a Service***
- Kontroluj dostęp aplikacji kontenerowych uzyskujących dostęp do pamięci trwałej
- Brak zmian w aplikacjach kontenerowych

Dodatkowe korzyści z rozszerzeniem Kubernetes

- Ochrona przed dostępem użytkowników root/uprzywilejowanych/nieautoryzowanych w kontenerach
- Chroń dane przed atakami eskalacji uprawnień z innych kontenerów
- Łatwo izoluj dostęp do danych między kontenerami
- Spełnij wymagania dotyczące zgodności w zakresie kontroli dostępu do danych i audytu na poziomie kontenera

CSI

THALES

Jak możemy pomóc?

CipherTrust Transparent Encryption dla…

- Szyfrowanie danych (wrażliwych) na trwałym woluminie dołączonym do aplikacji kontenerowych. Co jest potrzebne: CTE-CSI + CM
- Szyfrowanie obrazów kontenerów (w spoczynku). Co jest potrzebne?: CTE+CM

Podpis cyfrowy

- „Pieczętowanie“ obrazu kontenera to kontroli integralności
  - Użyj podpisu cyfrowego aby podpisać obraz kontenera
  - Co jest potrzebne: HSM i nasze PS

HYOK dla „Google Cloud Run”

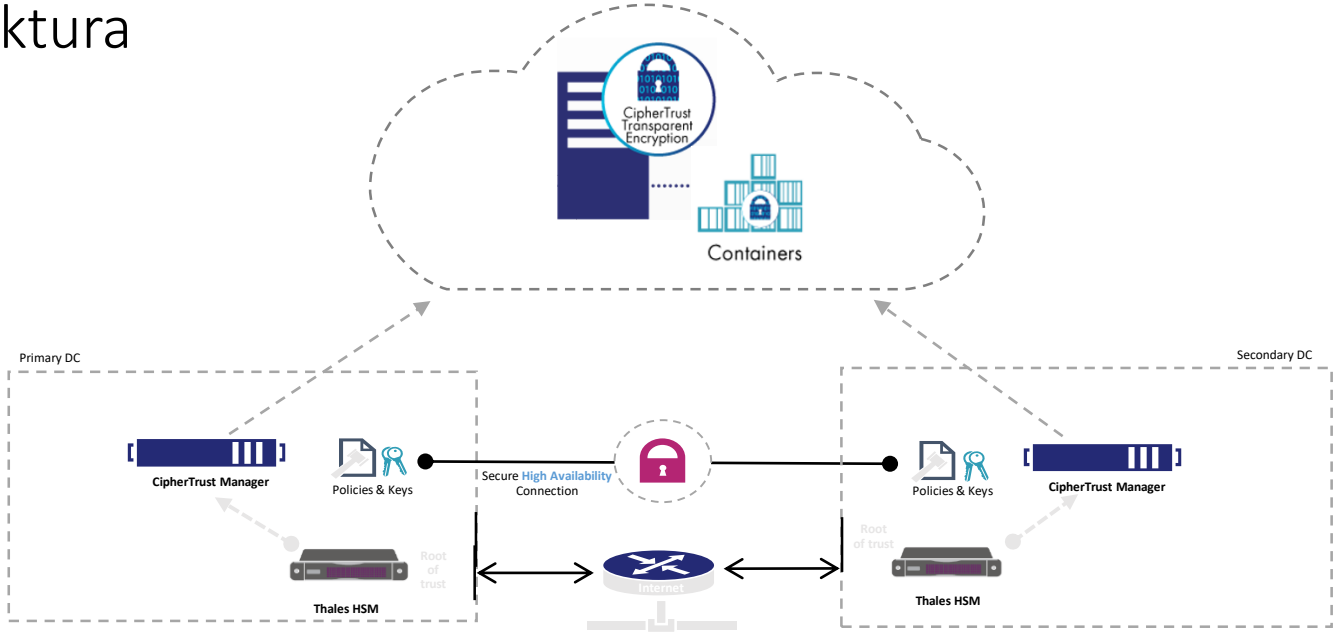
- Obraz kontenera może być zaszyfrowany kluczem klienta (więcej: tutaj)
- Co jest potrzebne?: CM z CCKM (Google EKMS)

THALES

CryptoPanel

podsumowanie

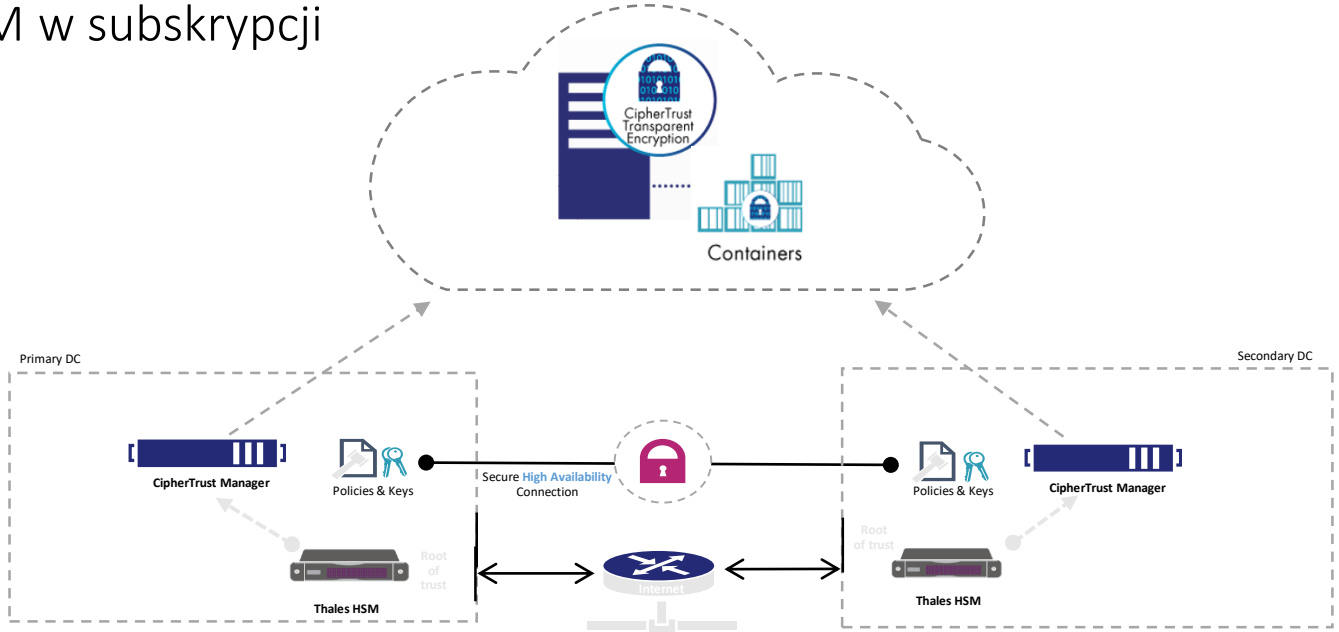
Architektura



- produkty dostępne w polskim kanale partnerskim
- model licencjonowania subskrypcyjny lub mieszany
- licencja demo do testów na 90 dni
- zalecane użycie HSM jako „root of trust”

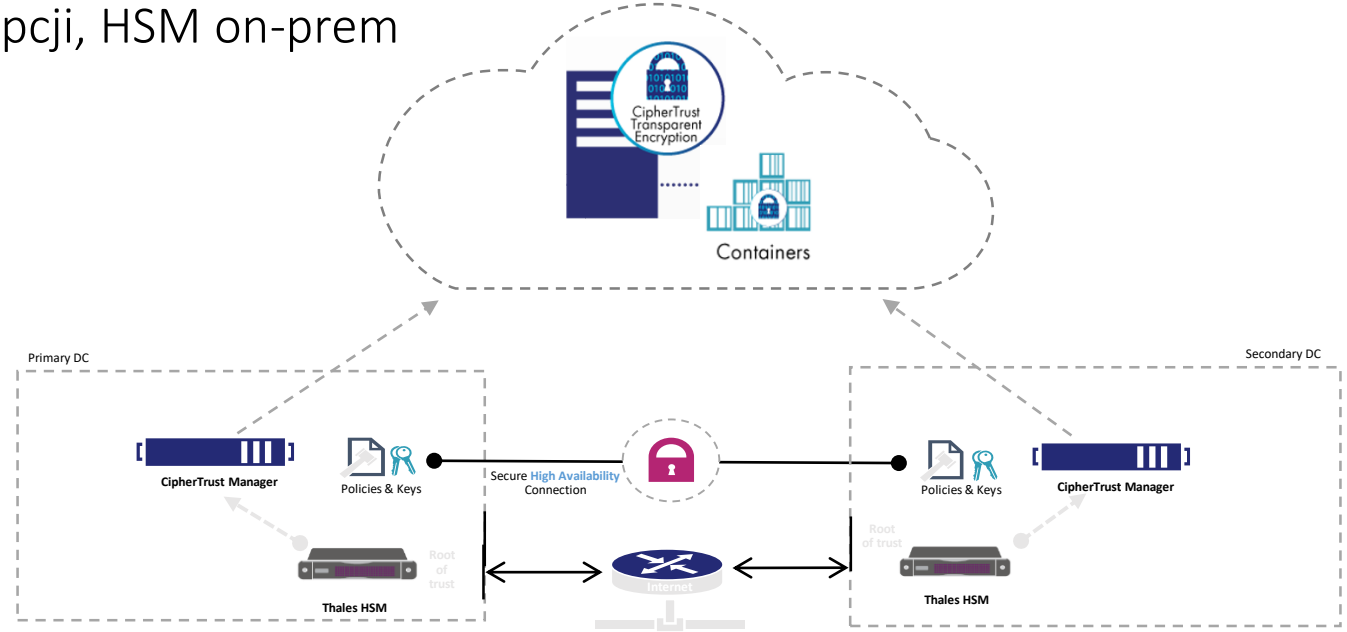
- Key Management System to *Thales CipherTrust Manager*
- Agent do integracji z OS z platformą konteneryzacji i Kubernetes to *Thales CipherTrust Transparent Encryption CSI (Container Storage Interface)*
- HSM to *Thales Luna seria A7xx lub seria S7xx*

CTE&CM&HSM w subskrypcji



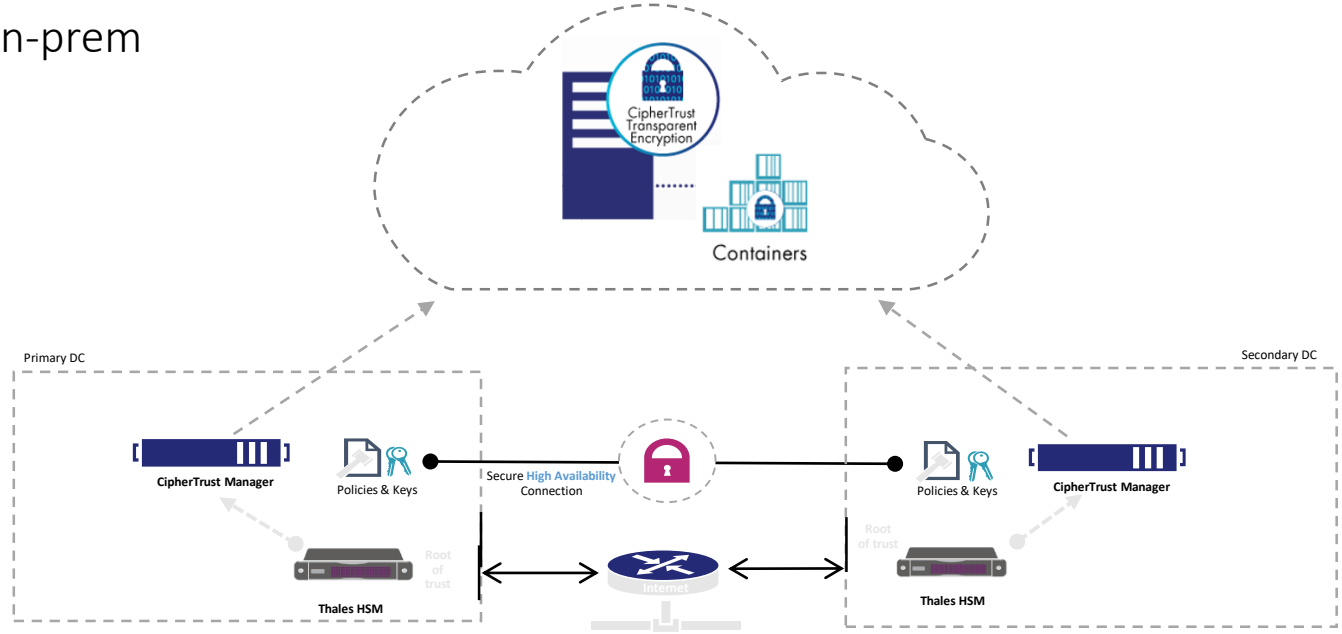
- **2x CipherTrust Manager – 2x 5,3k Euro netto - 12 miesięcy**
- **CipherTrust Transparent Encryption, Flex Connector Premium (1x instancja OS) – 5,5k Euro netto – 12 miesięcy**
- **Thales DPOD – Luna cloud service – 690 Euro netto – 1 miesiąc**

CTE&CM w subskrypcji, HSM on-prem



- **2x CipherTrust Manager – 2x 5,3k Euro netto - 12 miesięcy**
- **CipherTrust Transparent Encryption, Flex Connector Premium (1x instancja OS) – 5,5k Euro netto – 12 miesięcy**
- **2x Luna A700 – 2x 19k Euro netto + maintenance (dodatkowo ok. 17%)**

CTE&CM&HSM on-prem



- **2x CipherTrust Manager (perpetual lic.) – 2x 14,4k Euro netto + maintenance (dodatkowo ok. 17%)**
- **CipherTrust Transparent Encryption, Flex Connector Premium (1x instancja OS) – 17,9k Euro netto + maintenance (dodatkowo ok. 17%)**
- **2x Luna A700 – 2x 19k Euro netto + maintenance (dodatkowo ok. 17%)**

„Nauczki“, czyli *lessons learned i „w dokumentacji nie znajdziecie“*

- Czas zmienić paradygmat myślenia o tworzenia aplikacji…
  - *Container Technology is for Applications Developers*
- Dobry wyjaśnienie czym jest CSI i jak działa w K8s:
  - https://www.computerweekly.com/feature/Container-storage-101-What-is-CSI-and-how-does-it-work
- Lista ponad 60 dostawców (sterowników) CSI dla Kubernetes
  - https://kubernetes-csi.github.io/docs/drivers.html
- Thales CTE-CSI Deploy
  - https://github.com/thalescpl-io/cte-csi-deploy

CryptoPanel