CryptoPanel

edycja #6

...And Microsoft For All...

Bezpieczeństwo środowiska VDI (Virtual Desktop Infrastructure) z wykorzystaniem modułu TPM (Trusted Platform Module) na przykładzie Windows 11 i vTPM.

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


...AND
MICROSOFT
FOR ALL
CBS
SONY
COMPACT
disc
DIGITAL AUDIO
25DP 5178
STEREO
JASRAC
PRODUCED BY METALLICA WITH FLEMMING RASMUSSEN ENGINEERED BY FLEMMING RASMUSSEN
MIXED BY STEVE THOMPSON AND MICHAEL BARBIERO
"THE PRINCE" Not produced. Engineered by Mike Clink and Toby 'Rage' Wright.
Rough mix by Flemming Rasmussen.
©1988 METALLICA
MS ADCA 5:00
MS SQL EKM 10:01
AZURE BYOK 21:05
W11 & TPM 22:30
O365 DKE 6:20
CDN... 3:20
ALL RIGHTS OF THE MANUFACTURER AND OF THE OWNER OF THE RECORDED WORK RESERVED UNAUTHORIZED PUBLIC PERFORMANCE, BROADCASTING AND COPYING OF THIS DISC PROHIBITED. CBS/SONY RECORDS, A DIVISION OF CBS/SONY GROUP INC. TOKYO JAPAN

CryptoPanel

problem

co nas boli...

- Jesteśmy firmą, korzysta z wirtualnych stacji roboczych
- Chcemy zaktualizować Windows 10 do Windows 11
- Microsoft wydał nową wersję systemu operacyjnego - Windows 11
- Zmieniła się zasada korzystania z TPM

- *„Microsoft wymusza na VMware korzystanie z zewnętrznego KMS”*

Posiadamy Vmware 6.7
Potrzebujemy oprogramowania dla KMS do szyfrowania dla virtualnych maszyn aby instalować windows 11 .
Jest to wymóg przy instalacji tego systemu.

Szyfrowanie będzie odbywać się z wykorzystaniem VMEncrypt
U klienta jest 1 Vcenter (3nody)

Pozdrawiam,

THALES

CryptoPanel

rozwiązanie

Nim podamy rozwiązanie, powiemy po co nam TPM…

Komputery nie dają nam żadnych ukrytych powodów, by im ufać

Jak to zmienić?

- Opracowano modułu TPM (Trusted Platform Module)

Tak więc moduł TPM to...

- „…**dedykowany mikrokontroler** zaprojektowany do zabezpieczania sprzętu za pomocą zintegrowanych kluczy kryptograficznych.”

Moduły TPM umożliwiają systemowi:

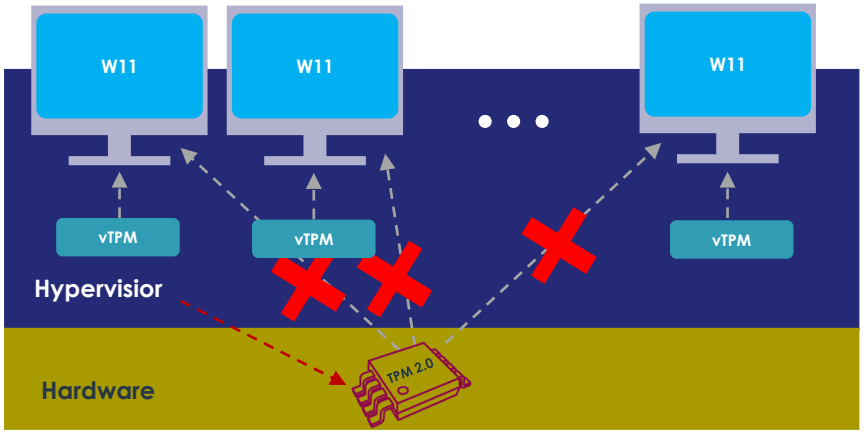
- Zebrać i potwierdzić stan systemu
- Przechować i generować dane kryptograficzne
- Udowodnić tożsamość platformy

Co jeśli na hoście działa hypervisor a VM również chcą korzystać z modułu TPM?

- Moduły TPM nie są zaprojektowane do zapewniania bezpieczeństwa więcej niż jednemu systemowi…

THALES

TPM a vTPM



vTPM dla środowisk zwirtualizowanych

VM nie mogą otrzymać dedykowanego mikrokontrolera…

- Zazwyczaj na hoście dostępny jest tylko jeden

Zatem vTPM

- vTPM, czyli „wirtualny Trusted Platform Module 2.0", pełni te same funkcje, co fizyczne urządzenie TPM 2.0, ale obsługuje funkcje koprocesora kryptograficznego w oprogramowaniu

Czy jest tak bezpieczny jak dedykowany mikrokontroler?

- Nie bo… patrz wyżej (podkreślone)

Czy vTPM jest to tylko funkcja w VMware?

Nie, to koncepcja, którą dostawcy wdrażają w swoich hypervisorach

A którzy dostawcy to robią?:

Citrix Hypervisor (XenServer)

VMware vSphere (ESXi)

Microsoft Hyper-V

…

THALES

Implementacja vTPM

Microsoft i VMware

Microsoft i VMware

Windows 10/11 & 2016

- Istnieją funkcje zabezpieczeń, które korzystają z modułu TPM

Jakie?

- Windows Defender Credential Guard
- Bitlocker
- …

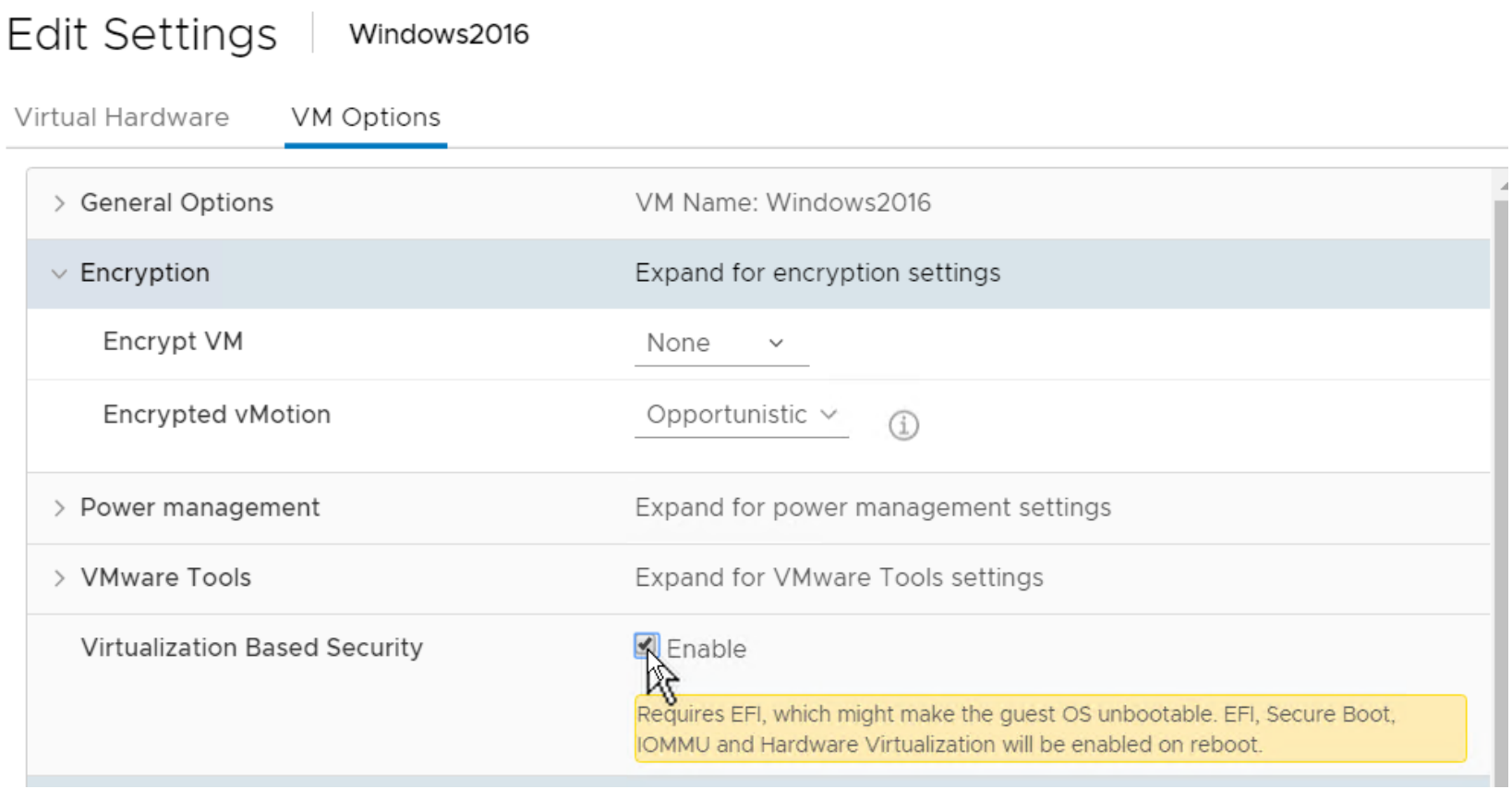
Windows 11 wymaga TPM 2.0 do instalacji *

- Zatem zrealizowanie VDI dla Windows 11 wymusza posiadanie vTPM

* - After initially claiming that Windows 11 won't work on a PC without a TPM **2.0** (or Trusted Platform Module), Microsoft has now confirmed to Tom's Guide that the OS actually requires only the older, much more common TPM 1.2 module — **but also that if you install Windows 11 on a machine without a TPM 2.0 chip, you'll be taking a risk.**

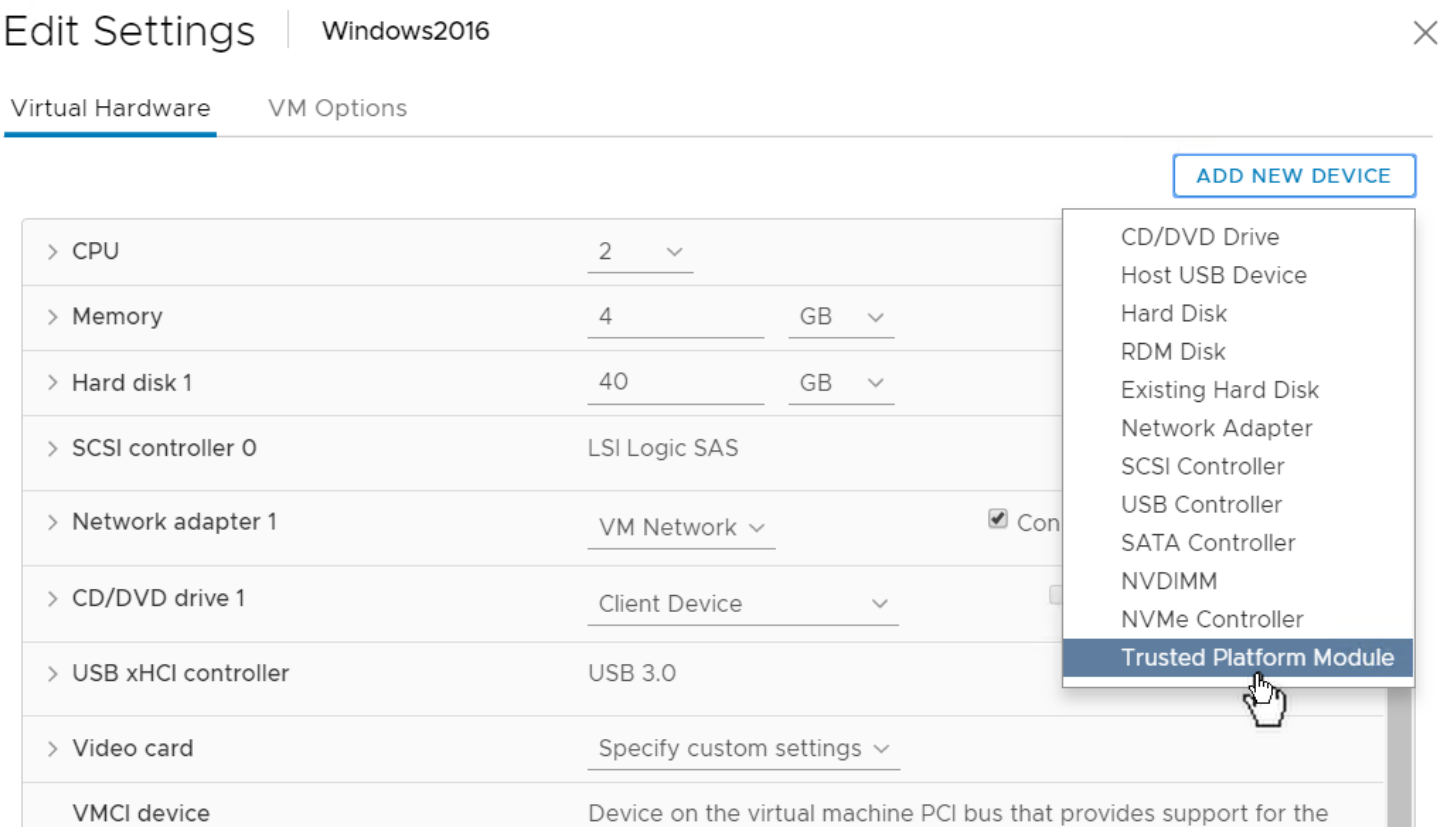
THALES

Po stronie VMware włącz: *Virtualization Based Security (VMEnrypt)*



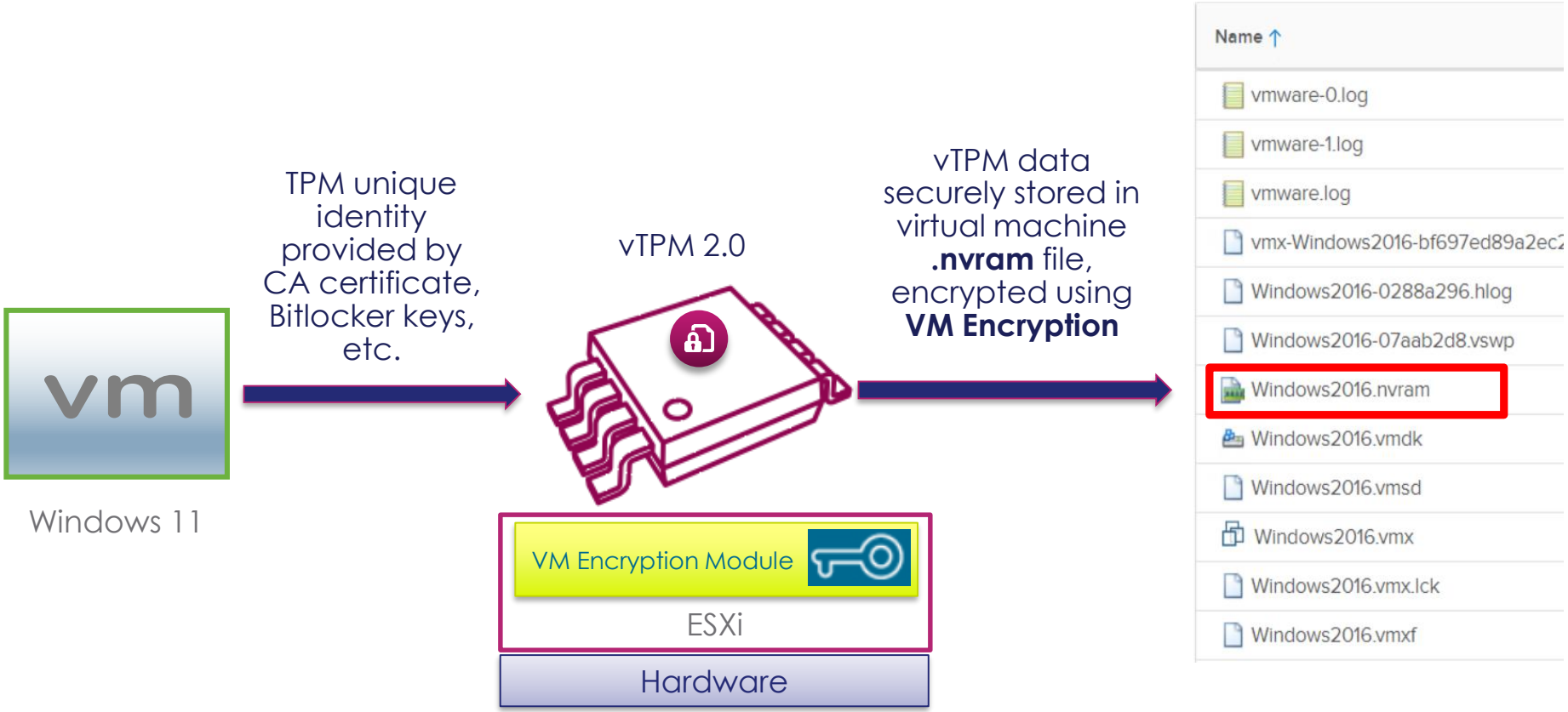
THALES

Dodaj vTPM do VM



THALES

Zabezpieczanie danych w vTPM



THALES

Zaszyfrowany *nvram* vs niezaszyfrowany?

.NVRAM Rozszerzenie pliku

Zweryfikowane

3.0 Popularność | Pliki danych

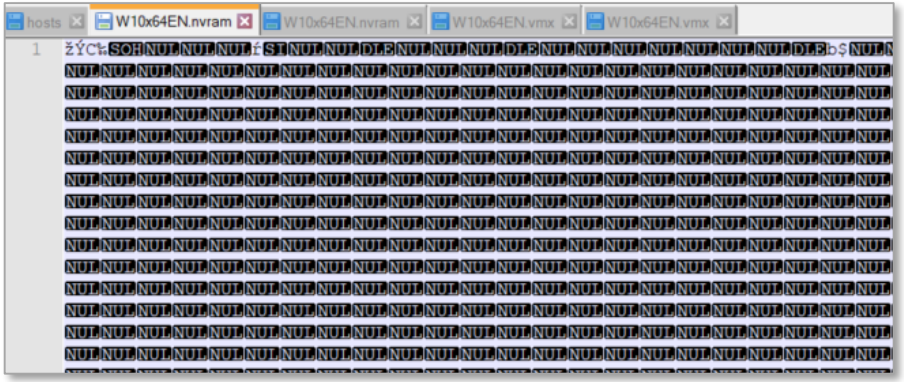
INFORMACJE O PLIKU NVRAM

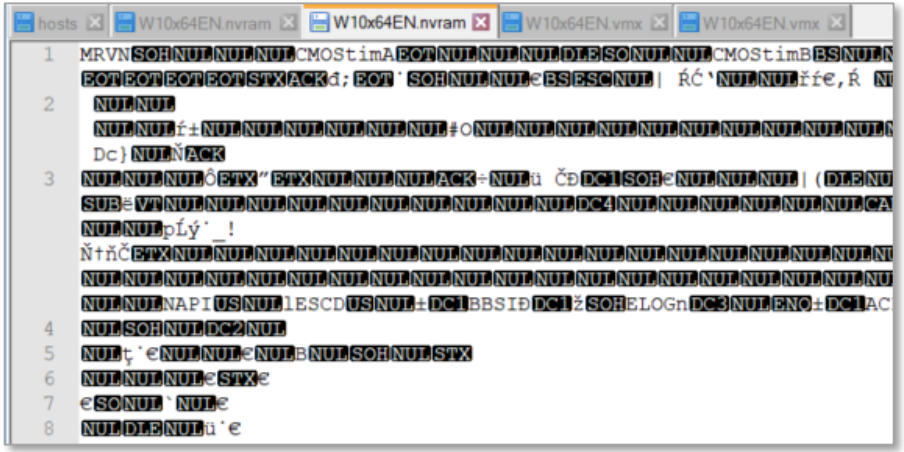
Typ pliku	VMware NVRAM Format
Kategoria pliku	Pliki danych
Wydawca	VMware

Czym jest plik NVRAM?

Rozszerzenie pliku NVRAM jest związane z oprogramowaniem do wirtualizacji VMware.

Plik NVRAM zawiera zapisany stan BIOS maszyny wirtualnej w formie podobnej do nieulotnej pamięci RAM - ogólne określenie pamięci, która zachowuje swoją zawartość po odłączeniu zasilania (lub rozszerzeniu za pomocą baterii zapasowej).

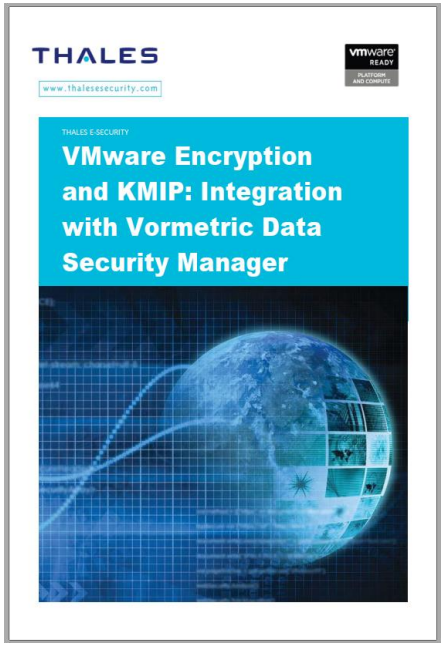




THALES

Thales i vTPM?

- Zawartość vTPM jest przechowywana w pliku `nvram` wraz z VM
- Ta zawartość jest szyfrowana za pomocą funkcji VM Ecryption przy hypervisora
- VM Ecryption musi mieć wdrożony zewnętrzny Key Manager *
  - np. CipherTrust Manager lub KeySecure



* https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-E5E8A9BF-F736-48D9-9DD4-A37F6333C692.html

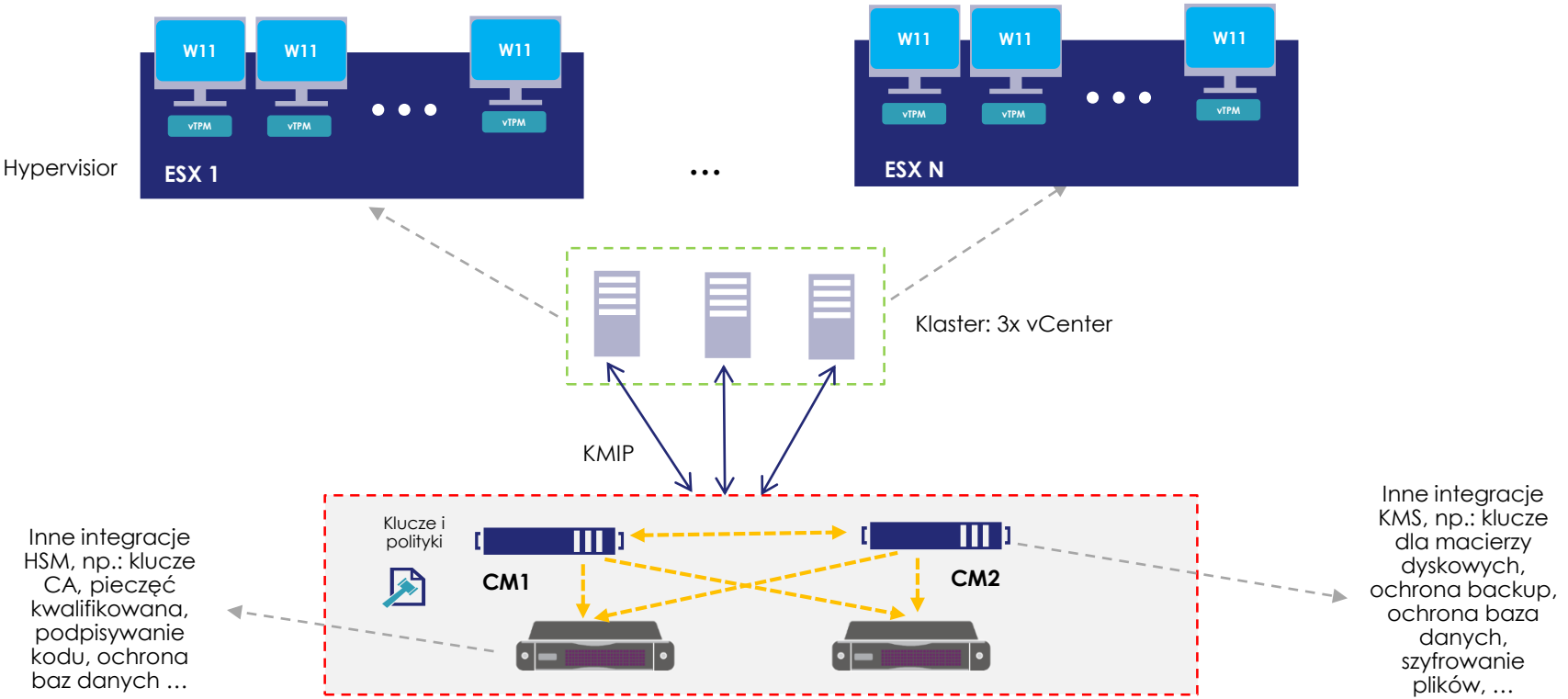
W11 -> TPM 2.0-> vTPM pod VDI -> szyfrowanie VM -> VMEncrypt -> extKMS -> Thales

THALES

…no a rozwiązanie?

Thales i Ty

Problem i propozycja



I słowo o tym „*co potrzeba*”?

- **CM szybko i łatwo integruje się z VMware (KMIP)**
  - Dostępny jako VM i HW
- **Dla wymagających:**
  - Możliwość wdrożenia klastra HA/LB oraz
  - Wzmocnienie ochrony dzięki *Root of Trust* (HSM)

- **produkty dostępne w kanale partnerskim**
- **licencja dożywotnia lub subskrypcja**
- **licencja demo do testów**
- **zalecane użycie urządzenia HSM**

Opcja 1

- **2x CipherTrust Manager – 14,5k € netto/szt**
- **3x KMIP Connector - 450 € netto/szt**

Opcja 2 na *wypasie*

- **J.w. plus:**
- **2x Luna A700 - 17,7k € netto**

CryptoPanel

podsumowanie

Podsumowanie

- Maszyny wirtualne mogą korzystać z modułu TPM za pośrednictwem vTPM
- vTPM wymaga skonfigurowania szyfrowania maszyn wirtualnych
- Z kolei szyfrowanie maszyn wirtualnych wymaga zewnętrznego menedżera kluczy, **w przeciwnym wypadku bądź świadomy ryzyka**.

- Czego potrzebujesz dla ochrony vTPM?
  - 2x CM - klaster niezawodnościowy KMS
  - Nx KMIP Connectors – dostawa kluczy do systemu zarządzania hypervisiora
  - Zalecamy: Root of Trust w postaci HSM (Luna lub DPoD)

THALES

Materiały

Oprogramowanie do pobrania lub wersja ewaluacyjna...

- Bardzo prosimy o kontakt z nami!

Dokumentacja:

- CipherTrust Manger: https://www.thalesdocs.com/ctp/cm/latest/
- Podecznik Integracji DSM-vCenter: https://cpl.thalesgroup.com/resources/encryption/vmware-encryption-and-kmip-integration-vormetric-data-security-manager-integration-guide

Zapraszamy także do obejrzenia CryptoPanel #4 posięwconego integracji vSphere i CipherTrust

- Link https://www.youtube.com/watch?v=m7Yp-6rTilM&list=PLjgNEisxn9fZfc48tMizrrGMrJG3PZQ7y&index=4

THALES

CryptoPanel