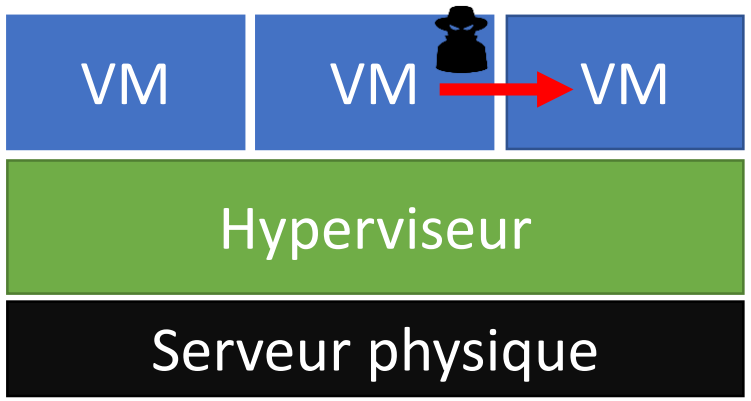
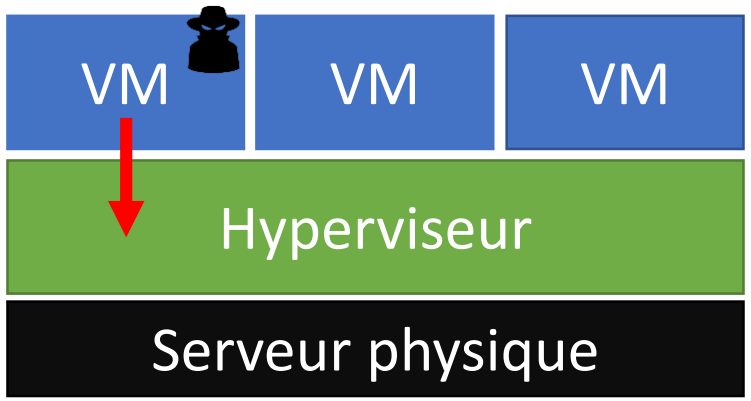
Machines virtuelles protégées

Jean-Baptiste Galet
SSTIC 2018 – 14 juin 2018

Introduction

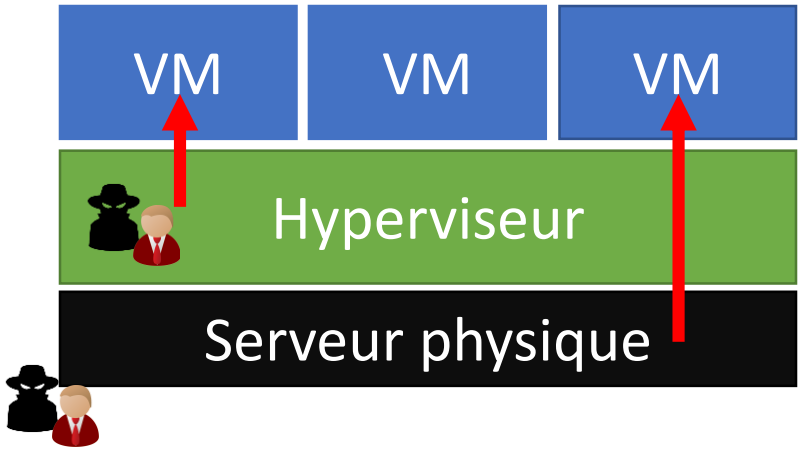


Guest to Guest

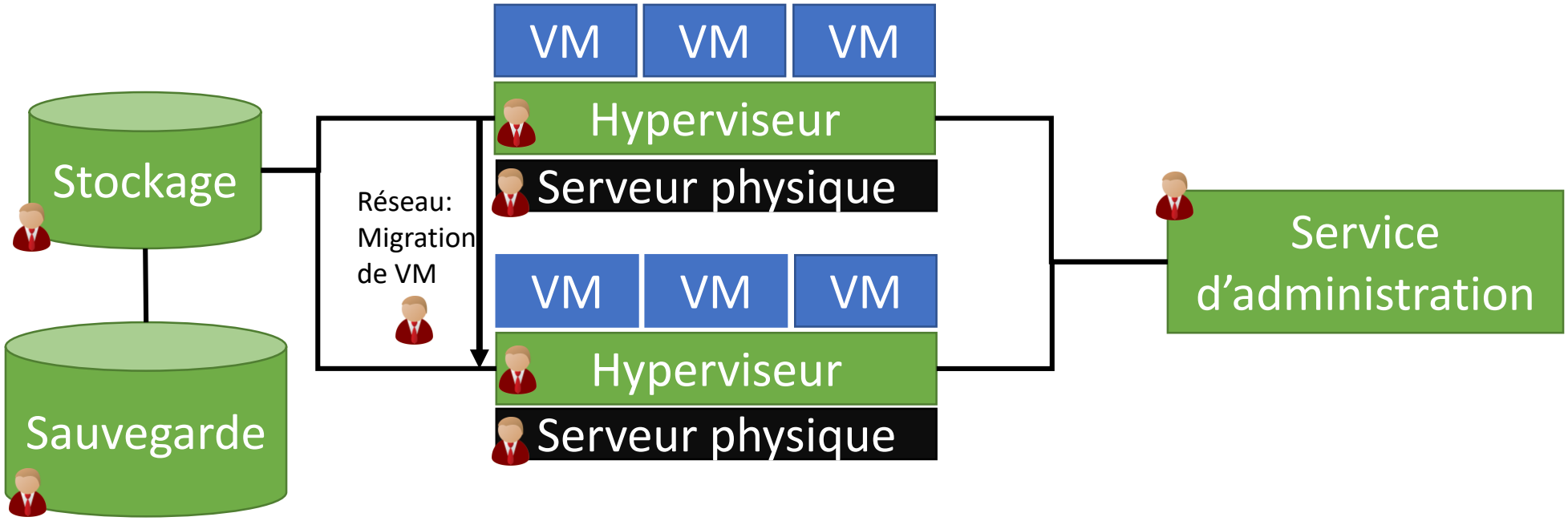


Guest to Host

Introduction



Introduction



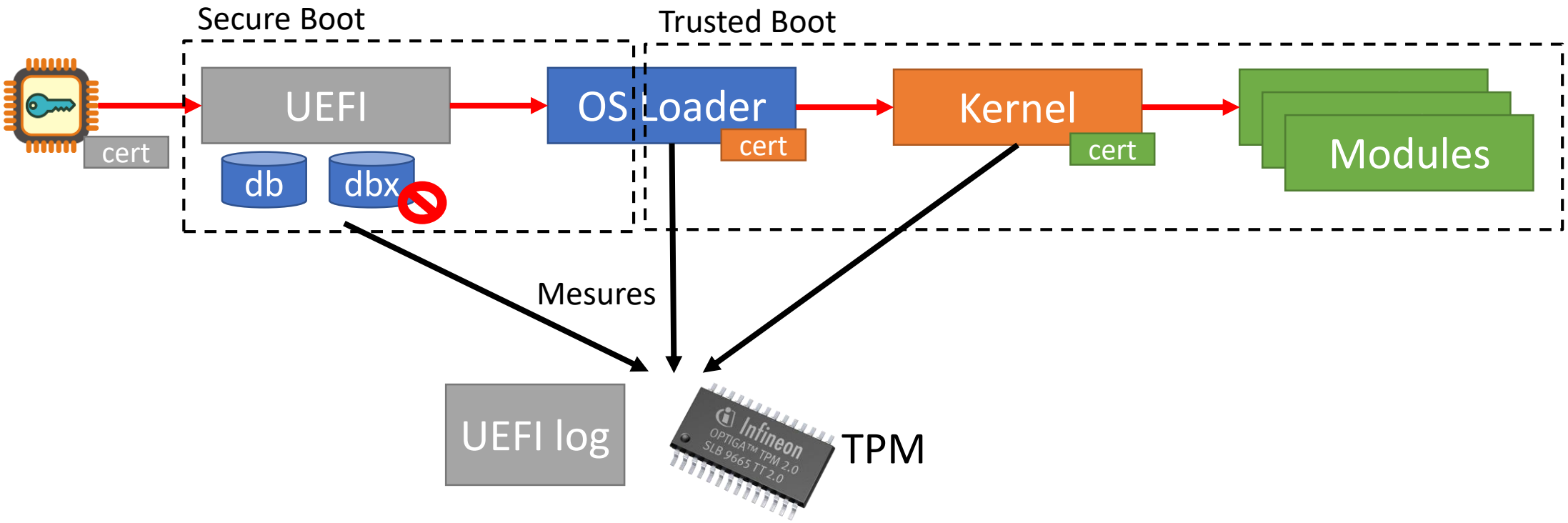
Introduction

Machine virtuelle protégée – Objectifs:

- Hyperviseur de confiance
- Séquence de démarrage de la VM intègre
- Disques chiffrés
- Snapshots chiffrés
- Mémoire vive protégée

- Migration entre hyperviseurs: trafic chiffré
- Accès à la machine (console, série, etc.) restreint

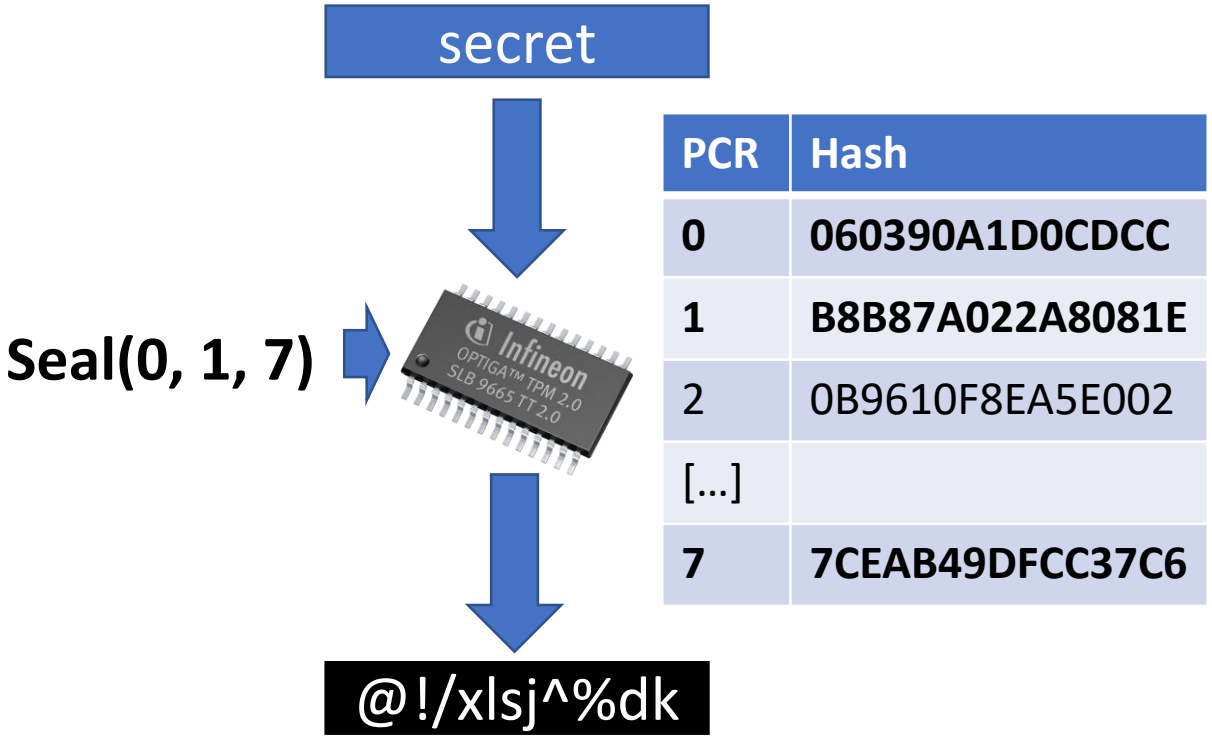
Démarrage sécurisé



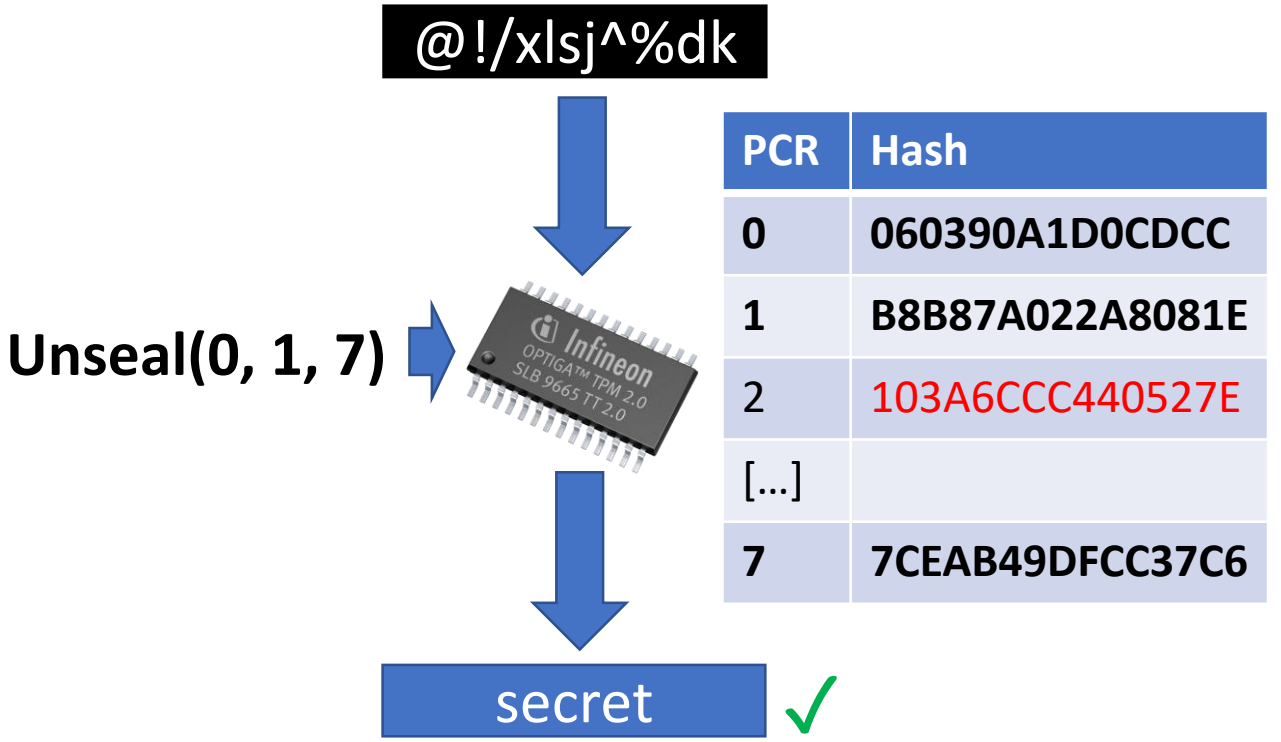
PCR: Registres de mesure du TPM

PCR_Extend(i, data) := PCR[i] ← HASH(PCR[i] || data)

TPM – Seal/Unseal



PCR	Hash
0	060390A1D0CDCC
1	B8B87A022A8081E
2	0B9610F8EA5E002
[…]	
7	7CEAB49DFCC37C6



PCR	Hash
0	060390A1D0CDCC
1	B8B87A022A8081E
2	103A6CCC440527E
[…]	
7	7CEAB49DFCC37C6

TPM – Remote Attestation

PCR	Hash
0	060390A1D0CDCC
1	B8B87A022A8081E
2	0B9610F8EA5E002
[…]	
7	7CEAB49DFCC37C6

PCR_Read([0, 1, 7]) := PCR[0] || PCR[1] || PCR[7]

Quote(KEY, [0, 1, 7]) := Sign(KEY, Hash(PCR[0] || PCR[1] || PCR[7]))

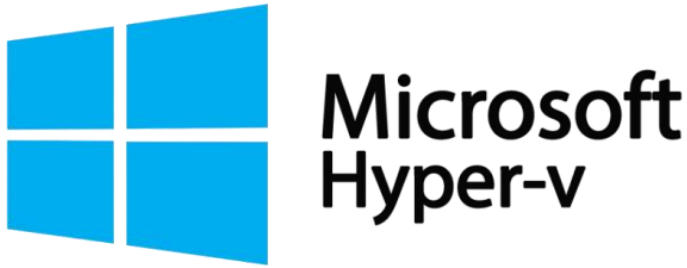
+ → Vérifications → **Attestation**

PCR	Data
0	08A84FE9625A0A6
0	EF9CD4DA9DD40F0
1	7DD004FDC3A5012
[…]	
0	10D4F4312080E048

UEFI log →

PCR	Hash
0	060390A1D0CDCC
1	B8B87A022A8081E
2	0B9610F8EA5E002
[…]	
7	7CEAB49DFCC37C6

Solutions



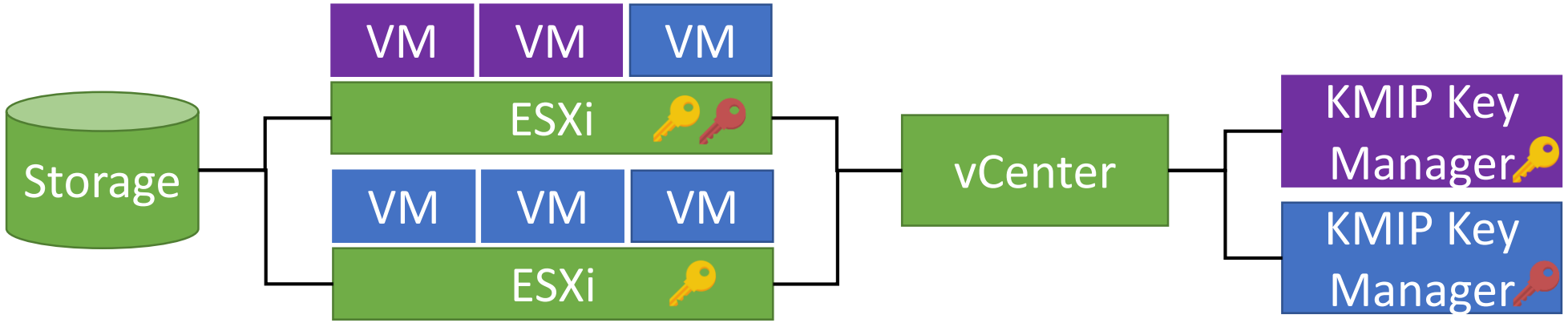
vSphere

6.5 (10/2016)

- ESXi Secure Boot
- VM Encryption
- Encrypted vMotion

6.7 (04/2018)

- TPM 2.0 – Attestation des ESXi
- Virtual TPM
- Support de VBS pour les VM Windows



vSphere

VM Encryption

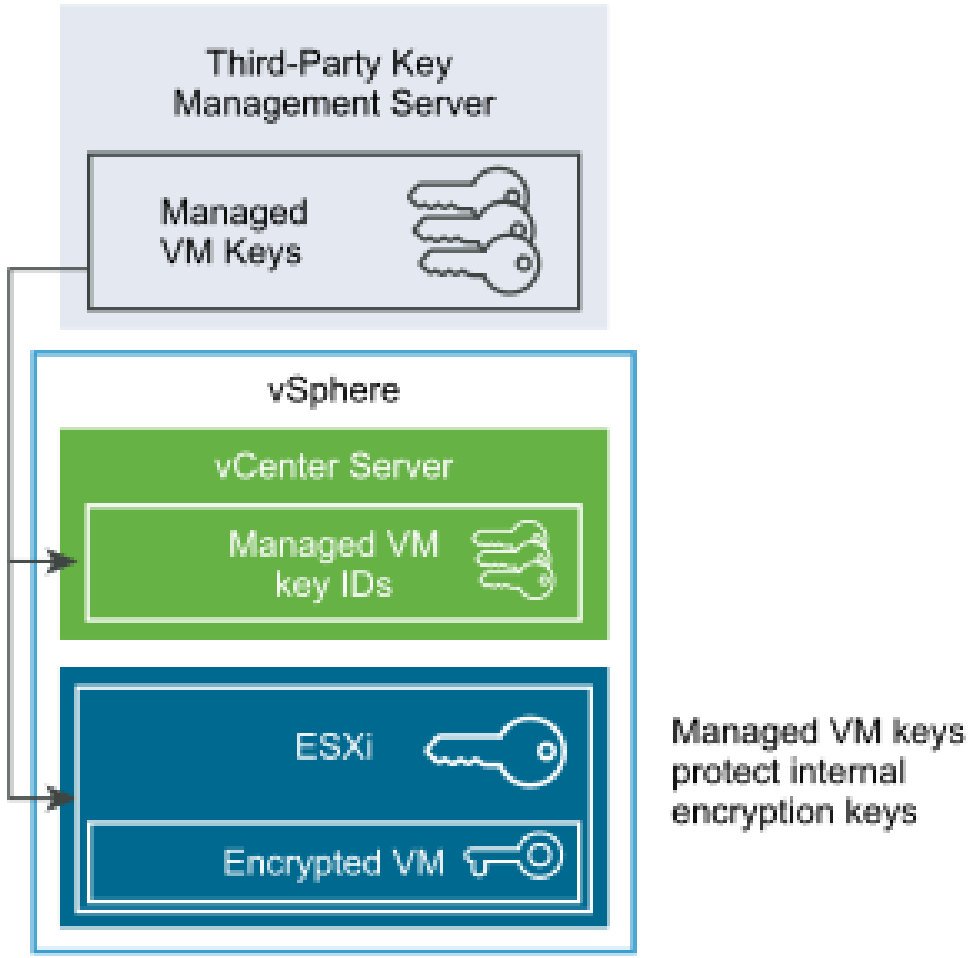
Chiffrement des disques virtuels (vmdk), des snapshots, des données de configuration sensibles (TPM)

2 clés utilisées:

- DEK (*Disk Encryption Key)*
  - Générée sur l'hyperviseur
  - Chiffrement des données
- KEK (*Key Encryption Key*)
  - Stockée sur le KMS
  - Chiffre les DEK

Encrypted vMotion

- Chiffrement applicatif
- Clé éphémère générée pour chaque migration



vSphere

Les KEK sont diffusées à tous les hyperviseurs du cluster

L'échec de l'attestation de l'hyperviseur n'empêche pas la diffusion des clés

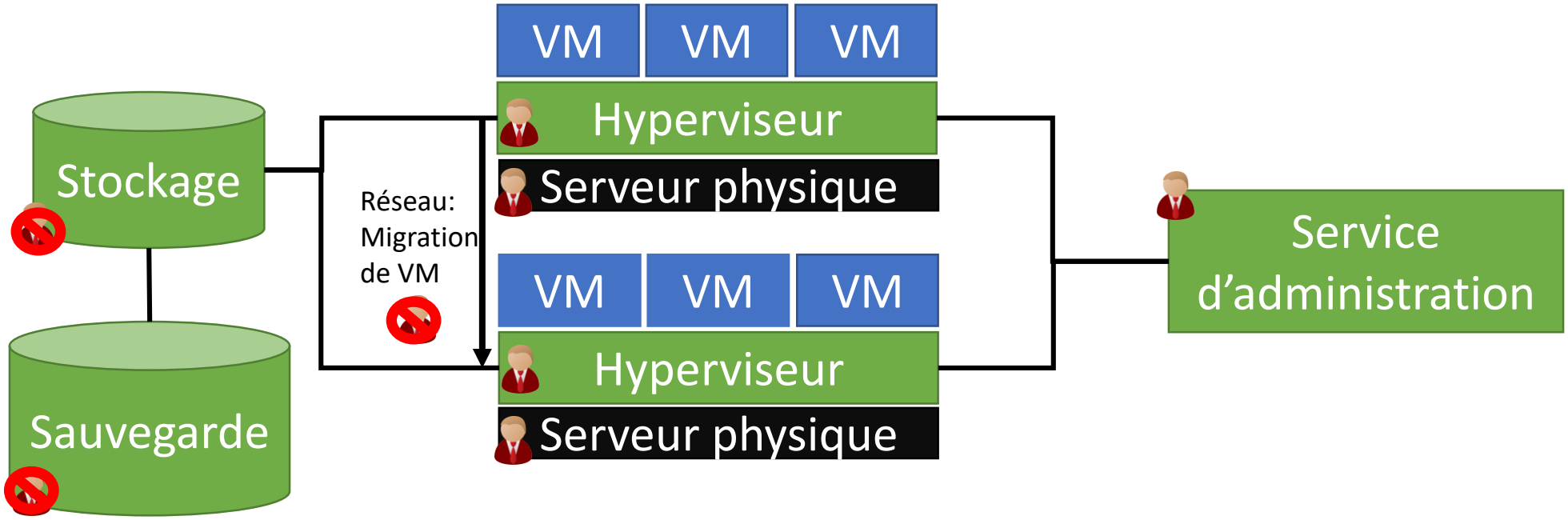
Les administrateurs locaux des hyperviseurs peuvent déchiffrer les données (`crypto-util`)

Some will ask questions such as "*But will this mean that VM's won't run on/vMotion to a host that has failed attestation?*". The answer is that VM's will continue to run on host that has failed attestation. What I can say in response is that "We are very aware of the ask for this capability" and we would really welcome your feedback.

https://blogs.vmware.com/vsphere/2018/04/vsphere-6-7-esxi-tpm-2-0.html

vSphere

Protections effectives

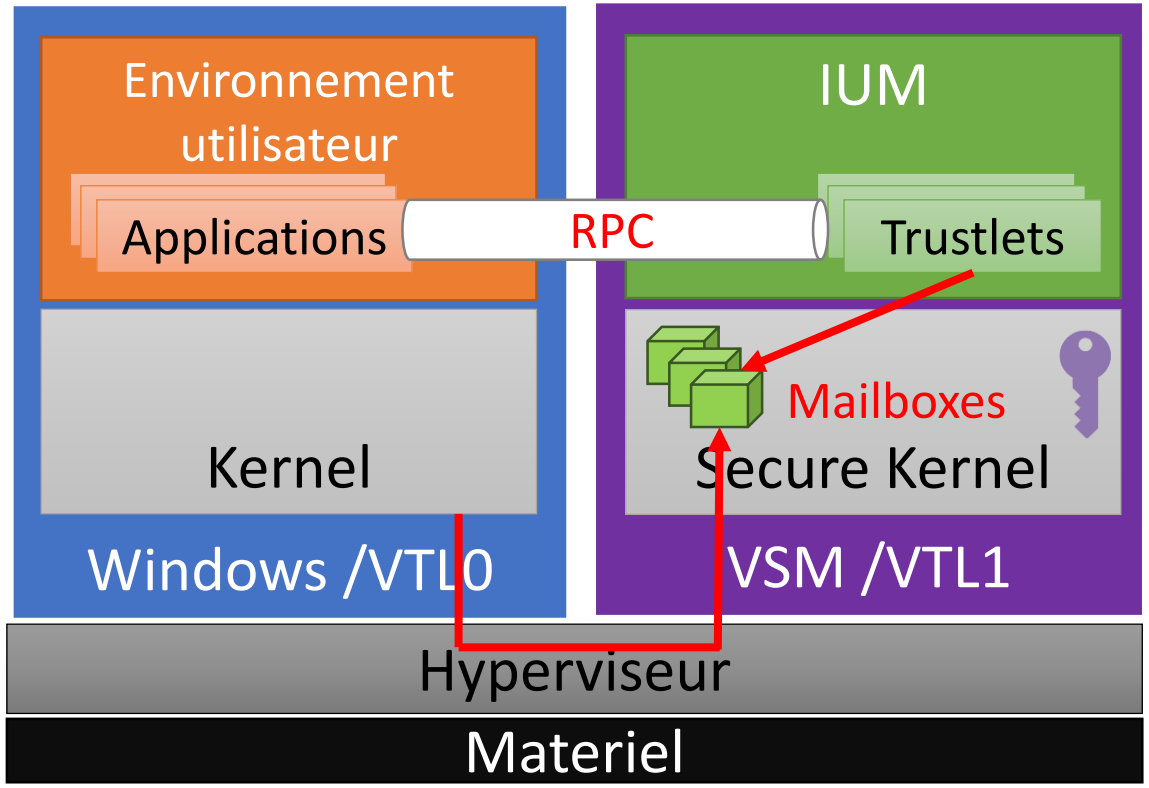


Hyper-V

- Windows Server 2016 (09/2016)
  - Introduction de *Guarded Fabric* (Rôles *Guarded Host* et *Host Guardian,* Shielded-VM)
- Windows Server / Windows 10 – 1709 (10/2017)
  - Ajout de la fonctionnalité *Guarded Host* sur les workstations
  - Support des Shielded-VM Linux
- Windows Server / Windows 10 – 1803 (04/2018)
  - v2 du protocole d'attestation à distance

Hyper-V

Virtualization-Based Security



Credential Guard

WDAC (*aka Device Guard*)

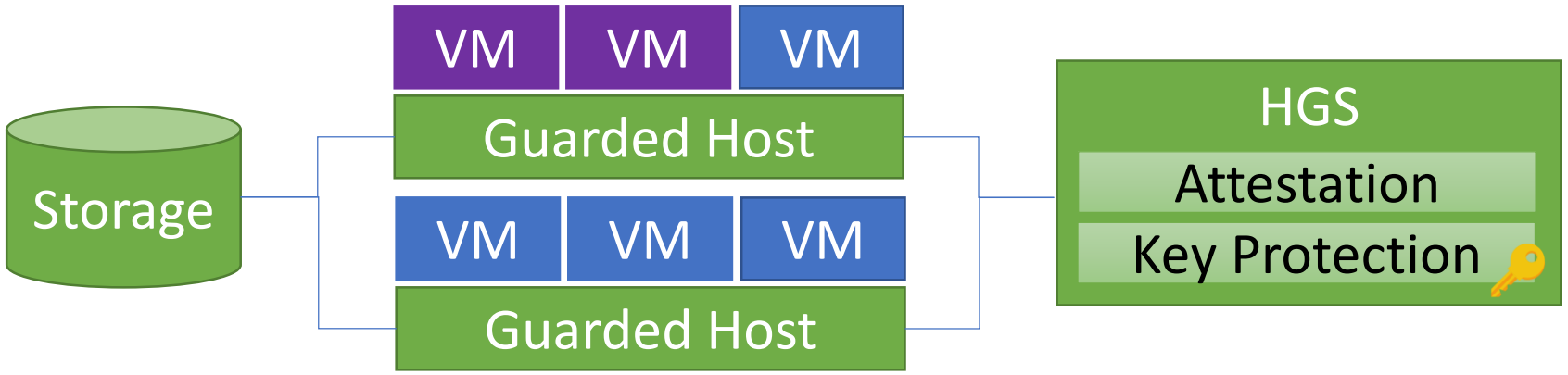
- Configurable Code Integrity
- HVCI

vTPM

VsmIdk : clé RSA scélée avec le TPM
Accessible uniquement par le VTL1

Hyper-V

- Guarded Host
  - Windows Server 2016 ou Windows 10
  - VBS + politique WDAC
- HGS (Host Guardian Service)
  - [Attestation Service] Réalise l'attestation des hyperviseurs
  - [Key Protection Service] Délivre les clés des machines virtuelles

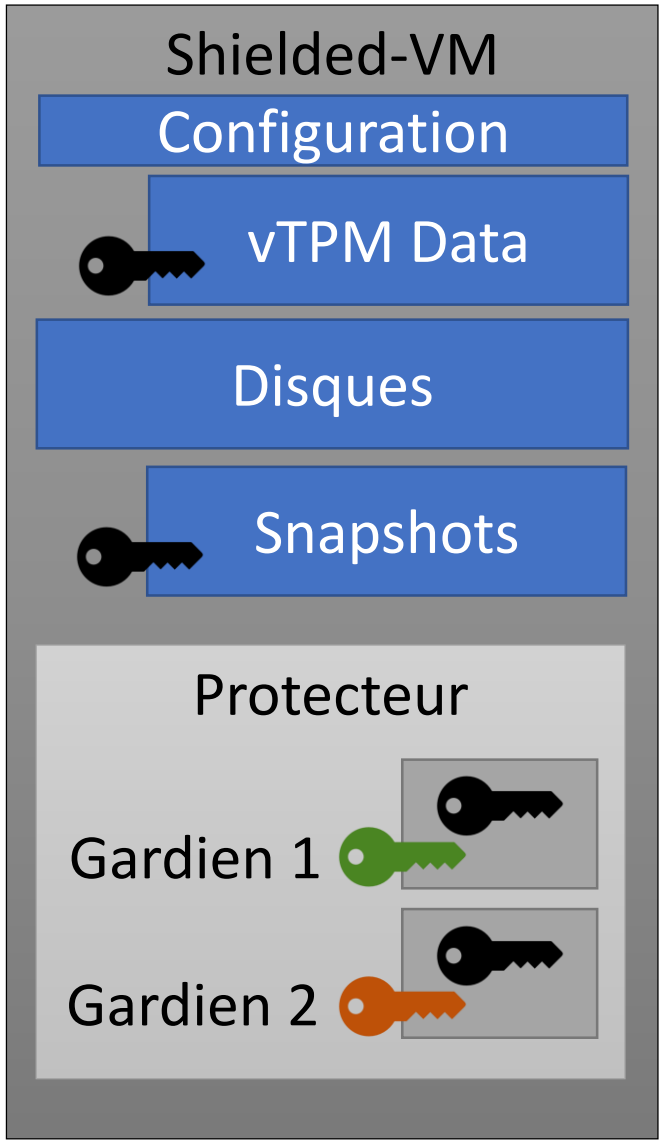


Hyper-V

Shielded-VM

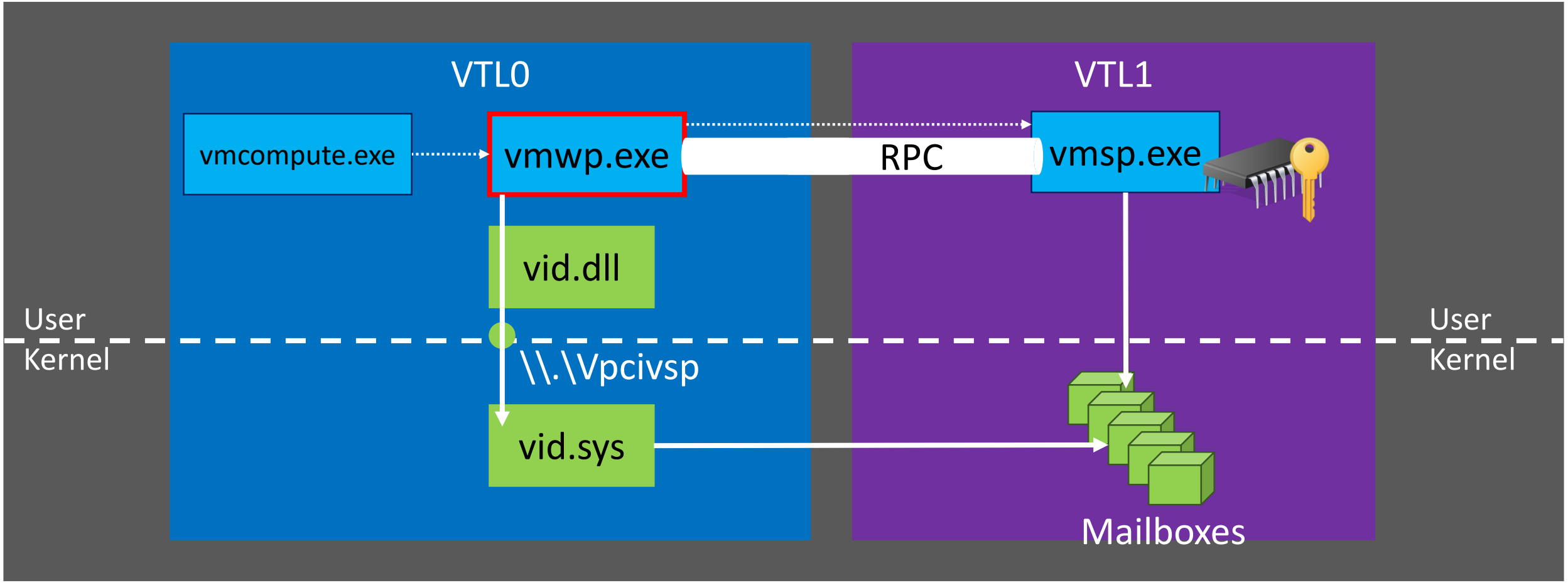
- Machine virtuelle avec:
  - UEFI + Secure Boot
  - TPM2 virtuel
  - Interfaces host – guest restreintes
  - Pas de console locale
  - Worker process en PPL
- La protection repose sur le chiffrement:
  - Du TPM virtuel
  - Des données volatiles pour les snapshots
  - Du trafic de live migration

Les données du disque doivent être chiffrées avec une solution FDE (Bitlocker / LUKS)



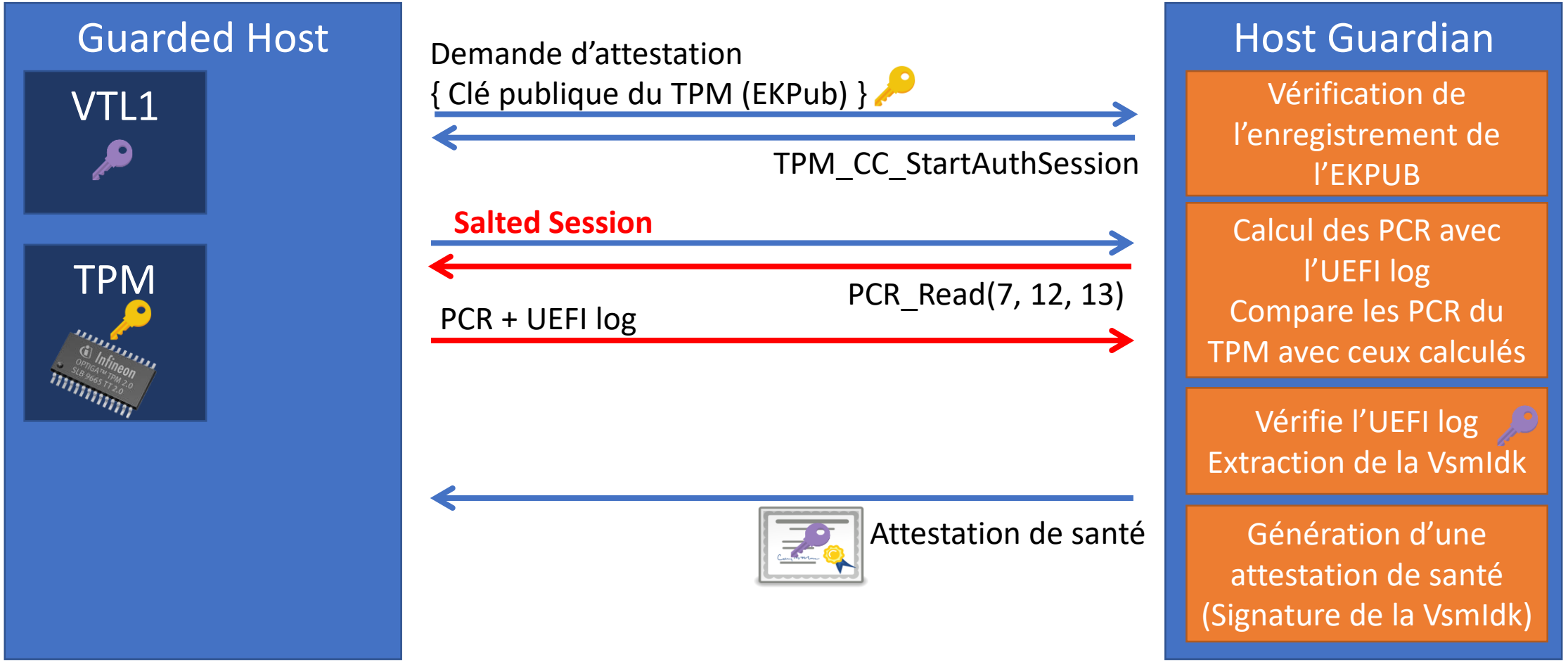
Hyper-V

Démarrage d'une Shielded-VM



Hyper-V

Attestation à distance (TPM)



Hyper-V

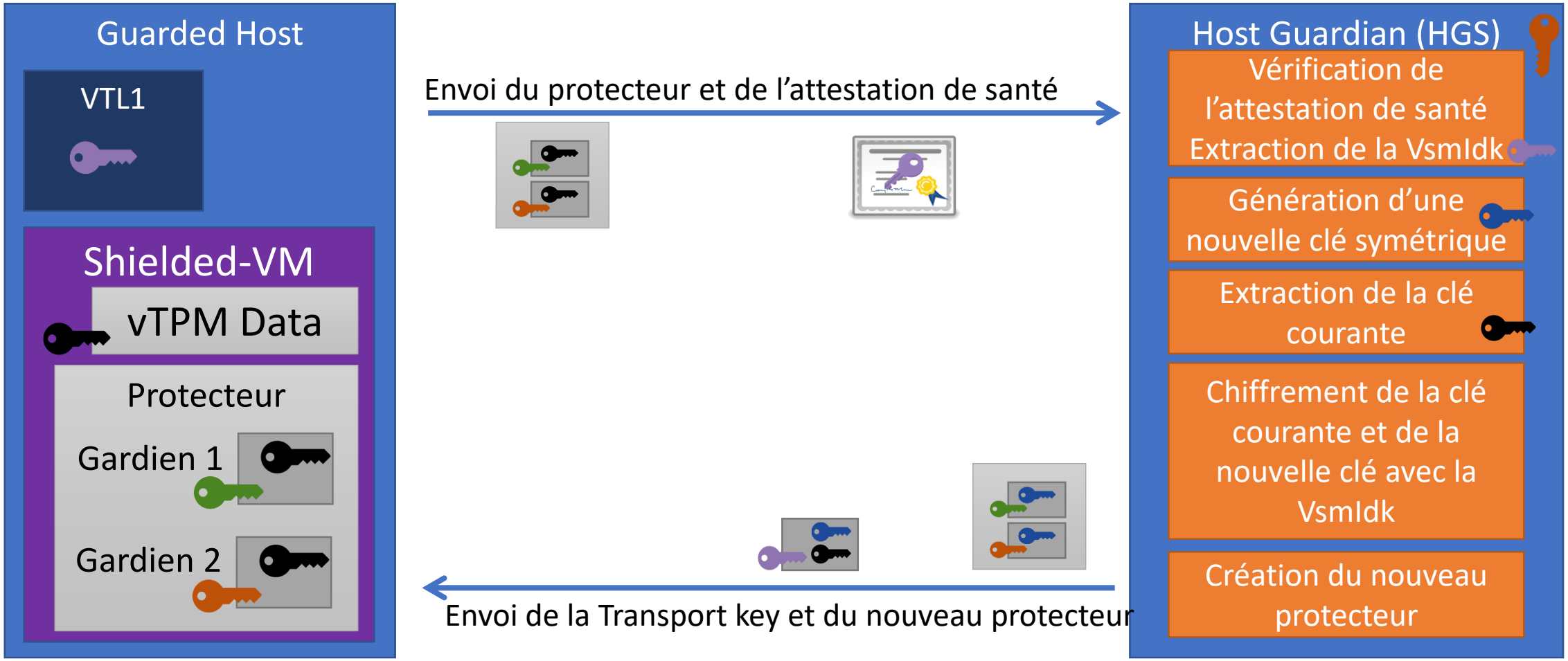
```
<EV_Event_Tag pcr="13" digest="BADD9A03D2FFB557B548D46E1E2C713A18B71A88">
  - <TrustBoundary>
        <ApplicationSvn>1</ApplicationSvn>
        <SvnChainStatus size="4">00000000</SvnChainStatus>
        <HypervisorDebug size="1">00</HypervisorDebug>
        <HypervisorIommuPolicy size="8">0100000000000000</HypervisorIommuPolicy>
        <HypervisorMmioNXPolicy size="8">0100000000000000</HypervisorMmioNXPolicy>
        <HypervisorMsrFilterPolicy size="8">0100000000000000</HypervisorMsrFilterPolicy>
        <BootDebug size="1">00</BootDebug>
        <TestSigning size="1">00</TestSigning>
        <FlightSigning size="1">00</FlightSigning>
        <CodeIntegrity size="1">01</CodeIntegrity>
        <BitLockerUnlock size="4">01000000</BitLockerUnlock>
        <MorBitApiStatus size="4">00000000</MorBitApiStatus>
      - <SIPolicy>
            <Version>10.0.0.0</Version>
            <Name>SiPolicy.p7b</Name>
            <Digest hashAlgorithm="SHA256">C0D67B1990FBBB6DCC97C9F823733F78829DE0659E3916081F9BE81483DBFAEA</Digest>
        </SIPolicy>
      - <LoadedModuleAggregation>
            <FilePath>\Windows\boot\resources\bootres.dll</FilePath>
            <ImageSize size="8">0070010000000000</ImageSize>
            <HashAlgorithmId size="4">0C800000</HashAlgorithmId>
            <AuthentiCodeHash size="32">CC0772C939B52DC46F716D4A6B1CE1C8552ADC1C812B702F635B98238C608F55</AuthentiCodeHash>
            <ImageValidated size="1">01</ImageValidated>
            <AuthorityIssuer>Microsoft Windows Production PCA 2011</AuthorityIssuer>
            <AuthorityPublisher>Microsoft Windows</AuthorityPublisher>
            <AuthoritySerial size="19">3300000173303107266 5B8B9B3000000000173</AuthoritySerial>
            <AuthoritySHA1Thumbprint size="20">14590DC5C3AAF238FCFD7785B4B93F4071402C34</AuthoritySHA1Thumbprint>
        </LoadedModuleAggregation>
```

Hyper-V

```
<PolicyElement id="96aa708e-5eff-4f9e-a2fd-421c1dcf5c5f" pcr="7">
    <EventSet allowEmpty="true">/PlatformInfo/TcgLog/Wbcl[@hashAlgorithm="SHA1" or @hashAlgorithm="SHA"]/EV_EFI_Variable_Driver_Config
        [@pcr='7' and EfiVariableData[VariableName='d719b2cb-3d3a-4596-a3bc-dad00e67656f' and UnicodeName='dbx']][1]</EventSet>
    <Property>@digest</Property>
    <Operator>NotEqual</Operator>
    <Value type="hexBinary">9A9E2E6E7A579F309012A94C4FCB8F917CE02C31</Value>
</PolicyElement>
<PolicyElement id="cb4e2588-7ddc-4d25-8991-e7b4027c1865" pcr="7">
    <EventSet allowEmpty="true">/PlatformInfo/TcgLog/Wbcl[@hashAlgorithm="SHA1" or @hashAlgorithm="SHA"]/EV_EFI_Variable_Authority
        [@pcr='7' and not(@digest='9FC713B7248D99A1A0DB3D50C14EB9B4FF270721')]</EventSet>
    <Property>@digest</Property>
    <Operator>Any</Operator>
</PolicyElement>
<PolicyElement id="da8c023e-68ea-4947-a3d0-2f94c214c83f" pcr="12">
    <EventSet allowEmpty="true">/PlatformInfo/TcgLog/Wbcl[@hashAlgorithm="SHA1" or @hashAlgorithm="SHA"]/EV_Event_Tag/TrustBoundary
        [ApplicationSvn][1]</EventSet>
    <Property>ApplicationSvn</Property>
    <Operator>LessThan</Operator>
    <Value type="unsignedLong">1</Value>
</PolicyElement>
<PolicyElement id="2c320df3-14c3-44d5-969a-3fd96cb9d291" pcr="13">
    <EventSet>(/PlatformInfo/TcgLog/Wbcl/EV_Event_Tag[@pcr='13']/SIPolicy[Digest[@hashAlgorithm='SHA256']] |
        /PlatformInfo/TcgLog/Wbcl/EV_Event_Tag[@pcr='13']/TrustBoundary/SIPolicy[Digest[@hashAlgorithm='SHA256']])[last()]</EventSet>
    <Property>Digest</Property>
    <Operator>Equal</Operator>
    <Value type="hexBinary">C0D67B1990FBBB6DCC97C9F823733F78829DE0659E3916081F9BE81483DBFAEA</Value>
</PolicyElement>
```

Hyper-V

Diffusion des clés



Hyper-V

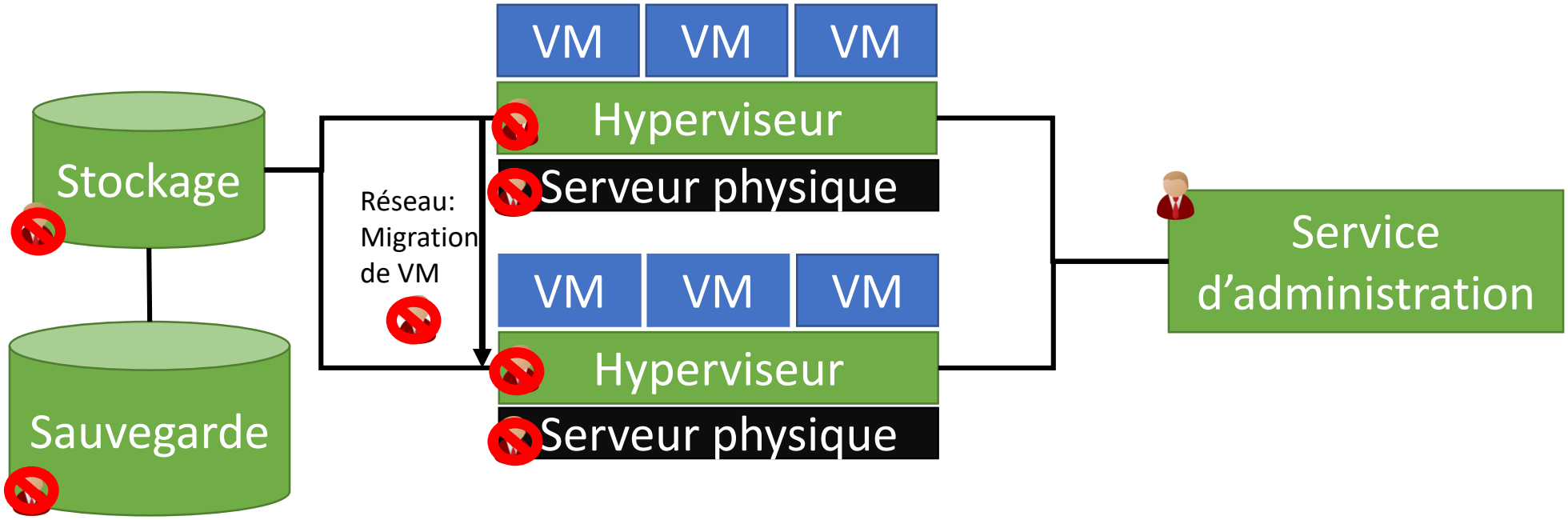
- L'attestation des hyperviseurs est limitée et manque de capacité de personnalisation
  - L'utilisation de Bitlocker avec un protecteur TPM permet de pallier cette limitation

- La *RAM* des machines virtuelles est accessible depuis le noyau du VTL0

- La sécurité des hyperviseurs repose fortement sur la politique WDAC
  - KMCI
  - UMCI: Nombreux bypass (*LolBins*)

Hyper-V

Protections effectives



Objectifs atteints ?

Machine virtuelle protégée

- ~ Hyperviseur de confiance
- ✓ Séquence de démarrage de la VM intègre
- ✓ Disques chiffrés
- ✓ Snapshots chiffrés
- ~ Mémoire vive protégée

- ✓ Migration entre hyperviseurs: trafic chiffré
- ~ Accès à la machine (console, série, etc.) restreint

Conclusion

- Les deux solutions présentées apportent des protections intéressantes
  - Ces protections restent perfectibles
  - Modérément complexe à mettre en œuvre
- Les éditeurs font évoluer ces fonctionnalités et communiquent dessus
- Des solutions matérielles émergent pour chiffrer la mémoire:
  - AMD SEV ⚠ *SEVered (Fraunhofer AISEC)*
  - Intel MKTME
- Travaux à poursuivre

Questions

@jbgalet