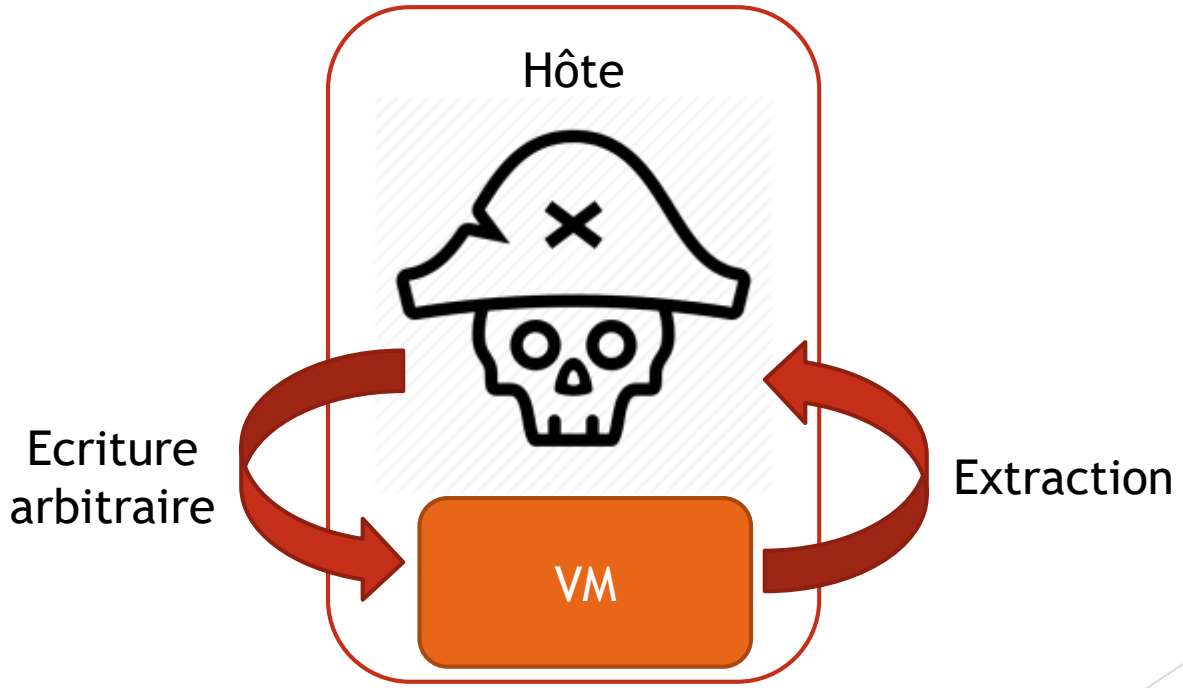
# Mécanismes de sécurité d'Hyper-V

Par Raphaël LOB

# Introduction

Lorsqu'un attaquant prend le contrôle de d'un hôte,
il peut aisément compromettre les machines virtuelles.

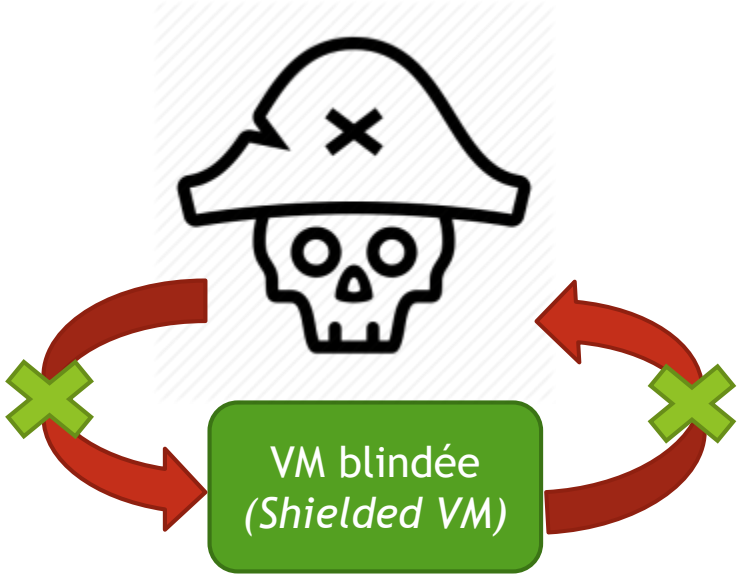


# Challenge

**Permettre une protection des machines virtuelles en cas de compromissions de l'hôte.**

1. Protection des données présentes sur les disques
2. Protection des données en mémoire

Hôte

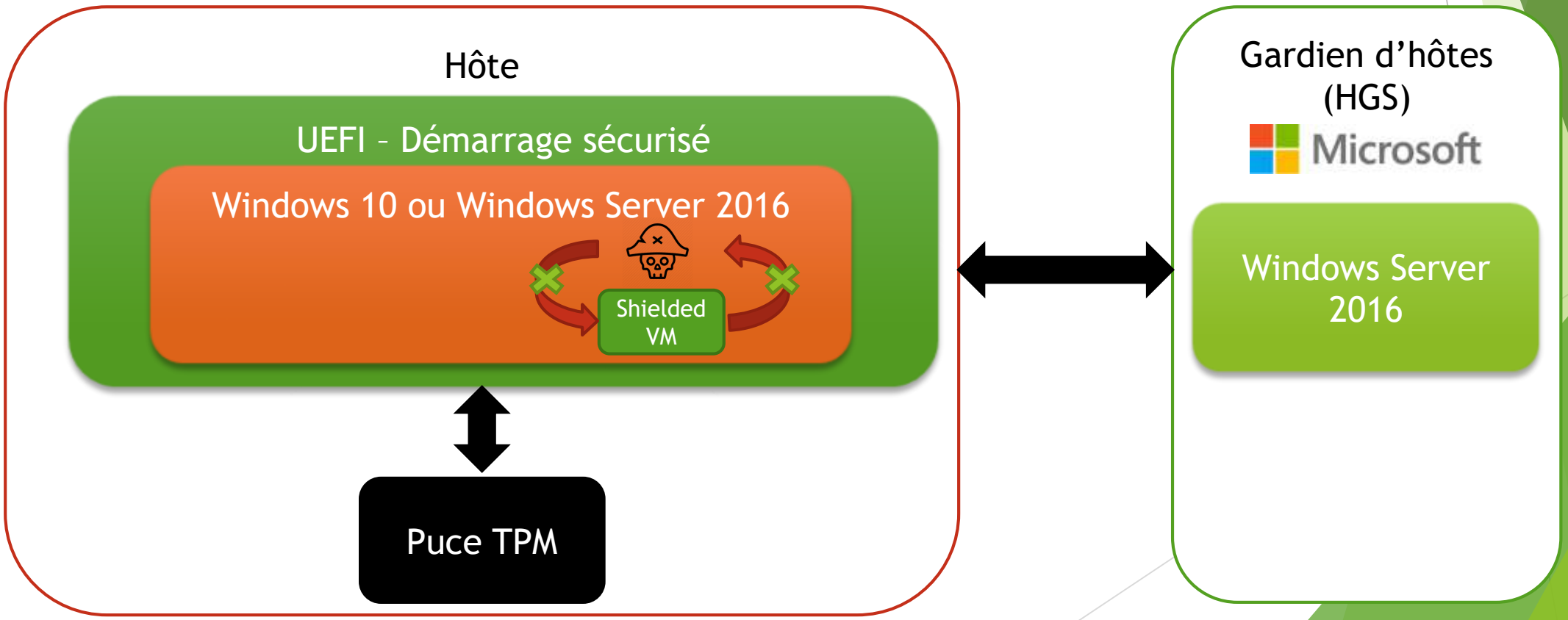


# Solution de Microsoft

**Système mise en place :**

- **Un hôte - Hyperviseur (Host);**
- Windows 10 ou Windows Server 2016
- UEFI avec démarrage sécurisé (Secure Boot);
- Puce TPM 2.0;
- **VT-X** activé (Extension processeur pour la virtualisation)

- **Un gardien d'hôtes (Host Guardian Services)**
- Windows 2016 Datacenter Edition;



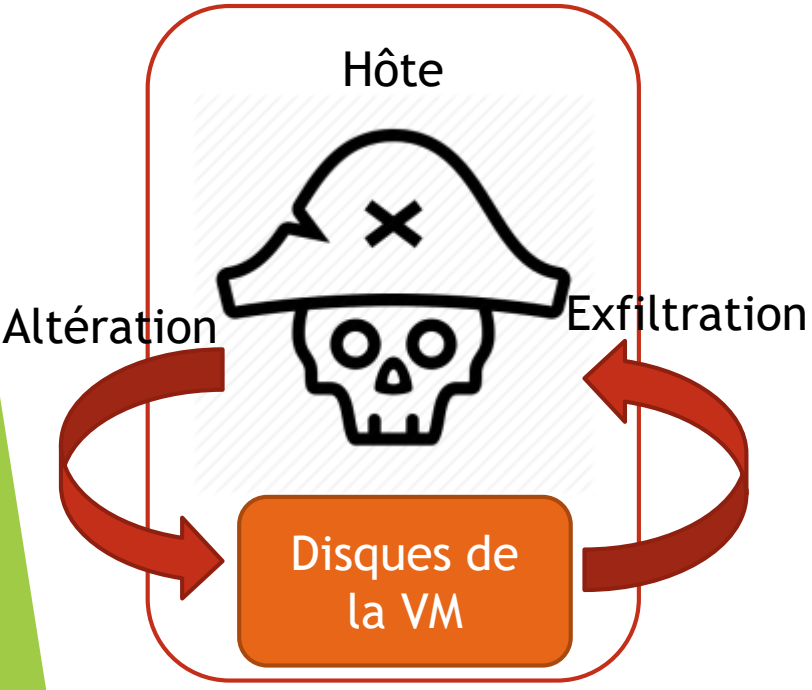
# Plan

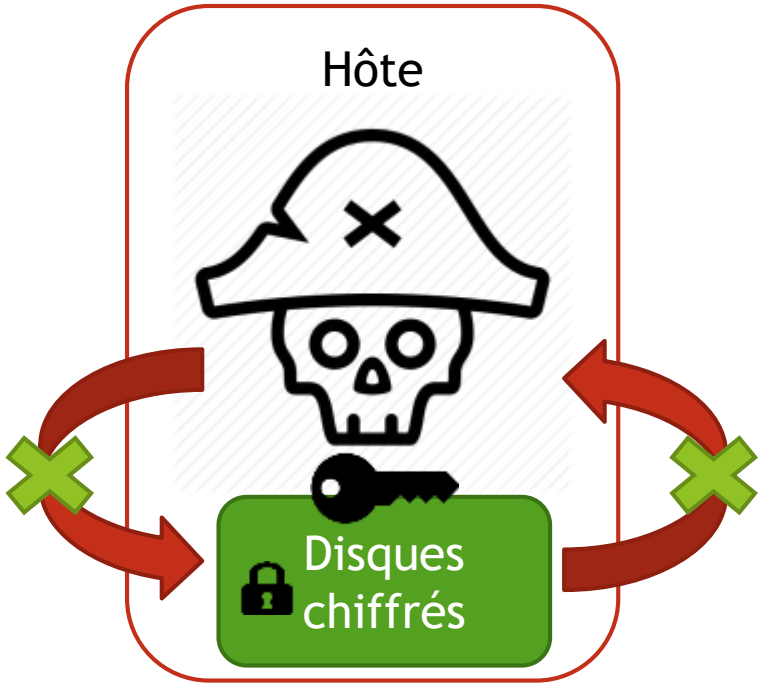
I. Idées globales
   I. Protection contres les attaques usuelles
   II. Attestation de santé
      I. Pendant la chaîne de démarrage
      II. Après la chaîne de démarrage
   III. Utilisation d'un tiers

II. Etudes approfondies des protocoles
   I. Protocole d'attestation de santé
   II. Protocole d'échange de clés
   III. Gestion des clés après réception

# Attaque usuelle : disque

**Permettre une protection des machines virtuelles en cas de compromissions de l'hôte.**




Gardien
*(Host Guardian Service)*

# Attaque usuelle : mémoire

**Restreindre l'accès de la mémoire**

Attaque Mémoire : Dump mémoire

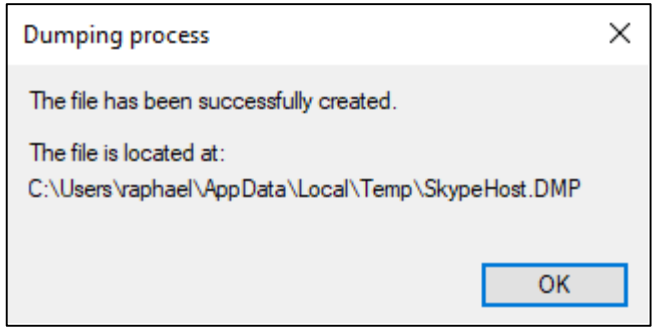
# Protected Process Light *(PPL)*

**Restreindre l'accès de la mémoire**

## Processus non protégé

Pas de restriction d'accès :

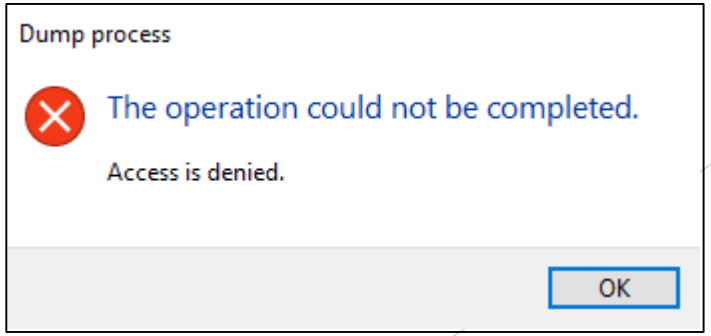
- Accès à la mémoire
- Injection de code
- Mettre en pause le processus
- Attacher un débugger
- Obtenir des informations sur les ressources utilisés




## Protected Process Light

Avec restriction d'accès :

- Pas d'accès à la mémoire
- Pas d'injection de code
- Pas de mise en pause
- Peu d'informations



# Protected Process Light *(PPL)*

**Restreindre l'accès de la mémoire**

Protected Process Light

Structure EPROCESS
Champ de niveau de protection :
Correspond au niveau de confiance de l'autorité ayant signé le processus

| Signer Name (PS_PROTECTED_SIGNER) | Level | Used For |
|---|---|---|
| PsProtectedSignerWinSystem | 7 | System and minimal processes (including Pico processes). |
| PsProtectedSignerWinTcb | 6 | Critical Windows components. PROCESS_TERMINATE is denied. |
| PsProtectedSignerWindows | 5 | Important Windows components handling sensitive data. |
| PsProtectedSignerLsa | 4 | Lsass.exe (if configured to run protected). |
| PsProtectedSignerAntimalware | 3 | Anti-malware services and processes, including third party. PROCESS_TERMINATE is denied. |
| PsProtectedSignerCodeGen | 2 | NGEN (.NET native code generation). |
| PsProtectedSignerAuthenticode | 1 | Hosting DRM content or loading user-mode fonts. |
| PsProtectedSignerNone | 0 | Not valid (no protection). |

Liste des niveaux de protections possibles

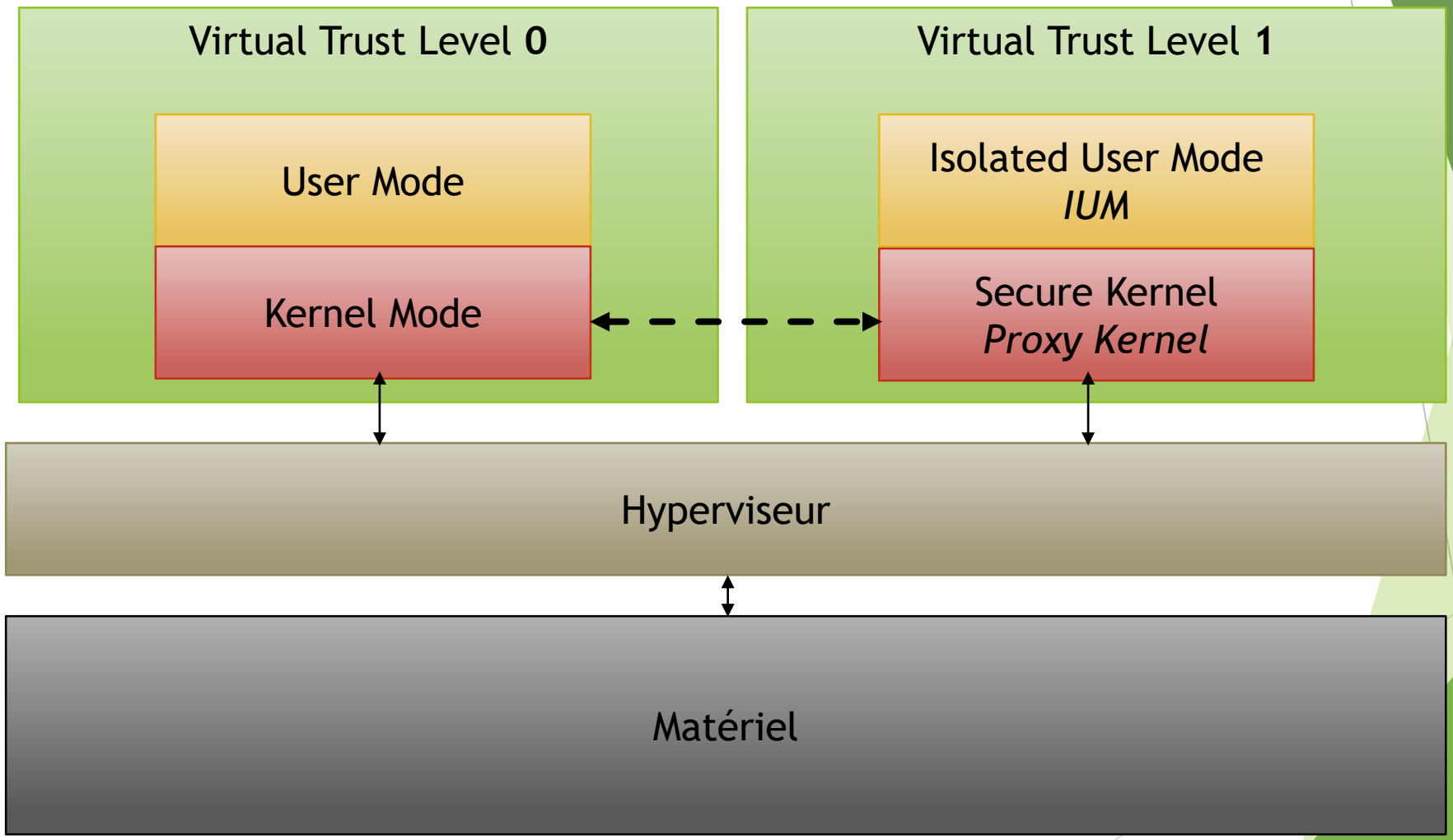
# Attaque noyau : mémoire

**Exécution de codes noyaux**

**Niveau noyau :** Modifie la valeur du champ de protection

# Virtual Secure Mode *(VSM)*

**Assurer une protection contre l'espace noyau**



# Mise en place des mécanismes mémoires

**Renforcer la sécurité des mécanismes d'hypervision**

| Process | PID | Description | Protection | Integrity | Path |
|---|---|---|---|---|---|
| vmcompute.exe | 3328 | Hyper-V Host Compute Service | | System | C:\Windows\System32\vmcompute.exe |
| vmwp.exe | 7688 | Virtual Machine Worker Process | | High | C:\Windows\System32\vmwp.exe |

| Type | Name |
|---|---|
| ALPC Port | \RPC Control\OLE186AC629610C3E38580B4474AAB8 |

Interaction entre hyperviseur et machine virtuelle non blindée

| Process | PID | Description | Protection | Integrity | Path |
|---|---|---|---|---|---|
| vmcompute.exe | 5116 | Hyper-V Host Compute Service | | System | C:\Windows\System32\vmcompute.exe |
| vmwp.exe | 7436 | Virtual Machine Worker Process | PsProtectedSignerWindows-Light | High | C:\Windows\System32\vmwp.exe |
| vmsp.exe | 6656 | | | High | [Invalid access to memory location.] |

| Type | Name |
|---|---|
| ALPC Port | \RPC Control\OLE973146DFC9462CF13203B354D109 |

Interaction entre hyperviseur et machine virtuelle blindée
vmwp.exe : PPL (Niveau de confiance 5)
vmsp.exe : Trustlet (Virtual Trust Level 1)

# Idée globale

**Permettre une protection des machines virtuelles en cas de compromissions de l'hôte.**

Déploiement de l'environnement blindé (à l'installation)

Echange des valeurs de références avec le gardien

Attestation de santé (Toutes les 8 heures)

*Admin Trusted* | *TPM Trusted*

Key Protection Service (Chaque démarrage de VM)

Mécanisme de récupération et de mise en place des clés

Hôte

VM blindée

Gardien

# Idée globale - Déploiement

**Permettre une protection des machines virtuelles en cas de compromissions de l'hôte.**

Hôte

Hyper-V

Gardien

Host Guardian Services

Certificats de signature et chiffrement

# Idée globale - Déploiement

**Permettre une protection des machines virtuelles en cas de compromissions de l'hôte.**

Hôte

Hyper-V


Mesures de références

Mesures de références

Gardien

Host Guardian Services

Certificats de signature et chiffrement

# Idée globale - Attestation

**Permettre une protection des machines virtuelles en cas de compromissions de l'hôte.**

Hôte

Hyper-V

VM blindée

Gardien

Host Guardian Services

Certificats de signature et chiffrement


Mesures de références

En cas d'expiration / d'absence de l'attestation

Demande d'attestation

Attestation de santé

Comparaison avec les mesures de références

Création d'une attestation de santé (Certificat X.509)

# Attestation de santé – Admin Trusted

**Contrecarrer les attaques plus sophistiqués : Confiance en l'administrateur**

Hôte

Hyper-V

VM blindée

Virtual Secure Mode

Demande d'attestation

Ticket Kerberos
*Virtual Secure Mode Identification Public Key*

Attestation de santé

Gardien

Host Guardian Services


Test appartenance à un groupe.

Création d'une attestation de santé
(Certificat X.509)

# TPM Trusted - Attestation de santé

**Contrecarrer les attaques plus sophistiqués : Ne pas faire confiance à l'administrateur**

1. Faire un relevé fiable la configuration de la machine
2. Durcir la politique d'exécution de codes

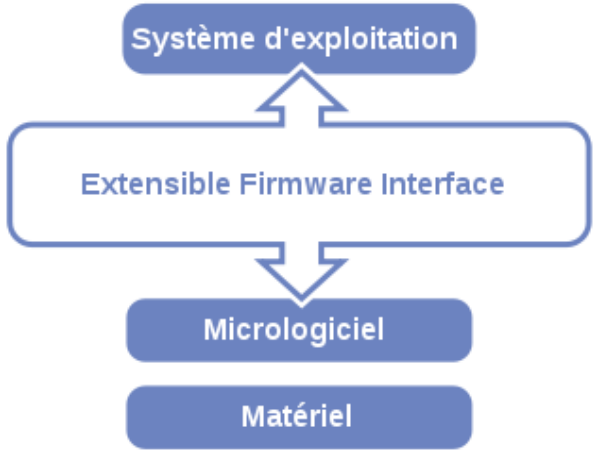
*Administrateur passant outre la sécurité du système.*

# La chaîne de démarrage

**Faire une mesure fiable des instructions chargées par les composants lors du démarrage**

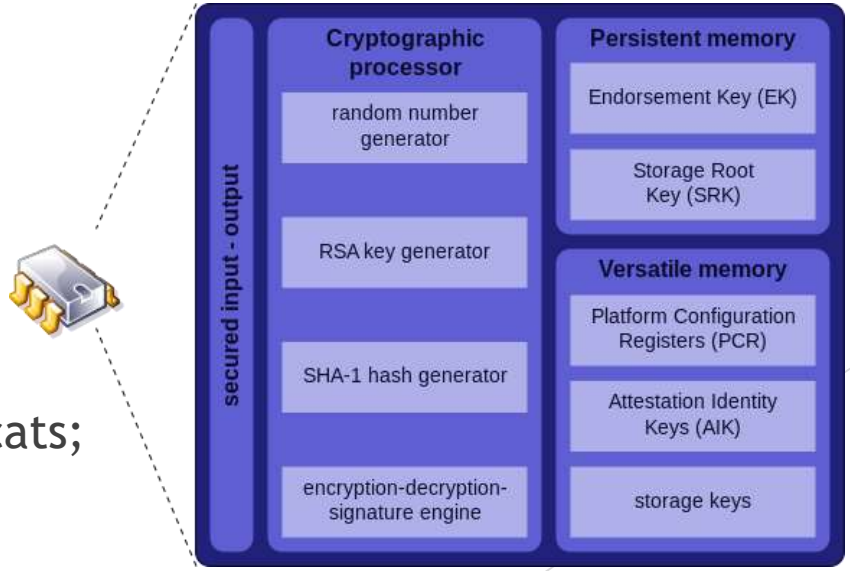
Utilisation de **UEFI 2.3.1+**

- Successeur du BIOS
- **Secure Boot** activé :
  - Ne charge que des **OS signés approuvés**



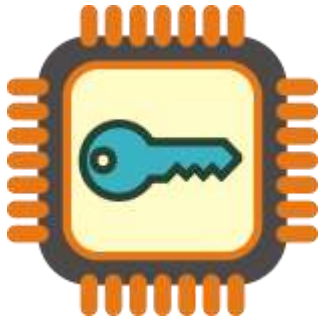

**Puce TPM 2.0**

- Puce indépendante;
- Identification du TPM; (Clé publique)
- Mesure (hachage) d'instructions;
- Attester de l'état d'une machine;
- Stocke des clés, mots de passes, certificats;
- Génère des nombres aléatoires;



# TPM - Platform Configuration Registers

TPM possède 24 Platform Configuration Registers (PCR) pour stocker le résultat de ses mesures. Ce sont des registres de 20 octets.



```
<PCRs>
  <PCR Index="00">efe1378096b63f97b4d839e98d47f9b9d55e8666</PCR>
  <PCR Index="01">22e5bd8826f235325d26535a94c0f08a4387b1c8</PCR>
  <PCR Index="02">241ca8d7fb91d036b987056655b67d1a970db531</PCR>
  <PCR Index="03">b2a83b0ebf2f8374299a5b2bdfc31ea955ad7236</PCR>
  <PCR Index="04">1e3c5e15b5f023765147535e092d22d7c17421e1</PCR>
  <PCR Index="05">5abb74776de1e0df65757d18a5d5a32de4bbc466</PCR>
  <PCR Index="06">b2a83b0ebf2f8374299a5b2bdfc31ea955ad7236</PCR>
  <PCR Index="07">772e490c1deca289ccb69f36098a2fff722a34b9</PCR>
  <PCR Index="11">ebb98df76613280f20dc38221143a9e727399486</PCR>
  <PCR Index="12">040ee435e43aff79f3a2382e1fbb46d0b24a4746</PCR>
  <PCR Index="13">8bc0bea7226d1bfb09bab89dd69187ef3f718820</PCR>
  <PCR Index="14">e70fbcbd5129cd3022cf8d52e04b9511dfc9c70e</PCR>
</PCRs>
```

Il n'existe pas de fonction SET sur un PCR, on peut seulement « *extend* » un registre en particulier .

$$PCR_{N+1} := H_{hashAlg}\left(PCR_N \,||\, data_{new}\right)$$

Possède des conditions pour effectuer des opérations (*Reset* / *Extend*) :

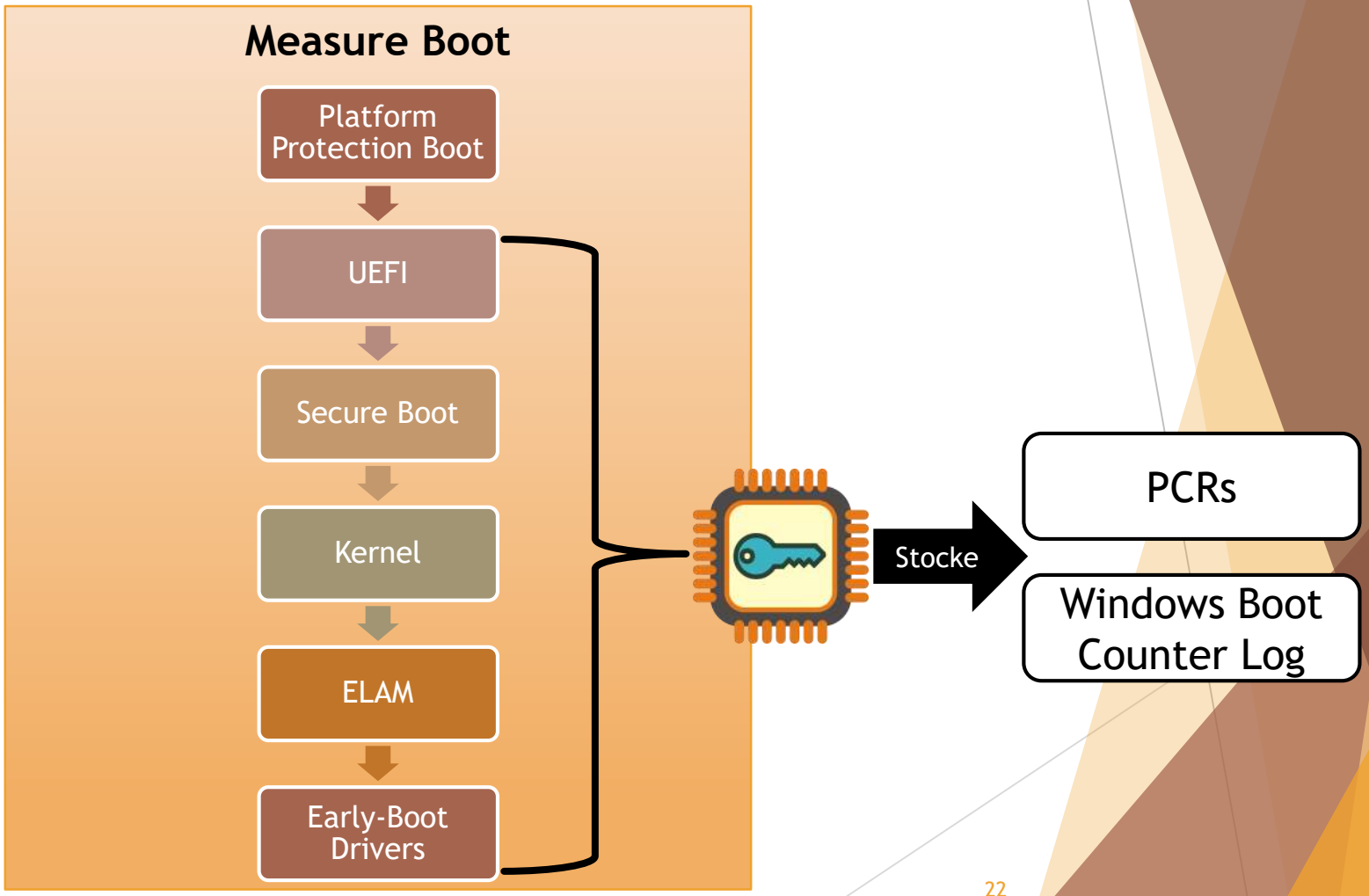
Certains PCR ne peuvent pas être remis à zéro que par un redémarrage du système.

Pour obtenir une mesure signée des PCRs, il faut effectuer une quote :

$$Quote(Nonce\ , PCRs(P), Clé\ d'attestation)$$

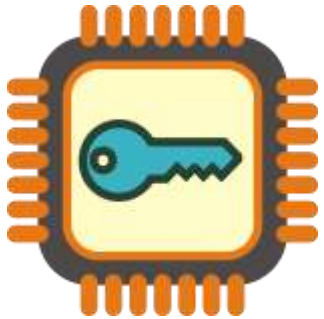
# Mesure de la chaîne de démarrage

**Faire une mesure fiable des instructions chargées par les composants lors du démarrage**



# TCGLog – WBLC

**Rendre la mesure du TPM exploitable**



Timeline
Chaine de démarrage

Baseline.bin

Via Powershell : Get-HgsAttestionBaselinePolicy -Path D:\Baseline.tcglog

Chaque rapport de démarrage est automatiquement stocké dans **%SYSTEMROOT%\Logs\MeasuredBoot**

Génère un blob d'environ 60ko :

- contient l'ensemble des instructions données au TPM;
- contient la valeur de chaque registre après chaque opération;
- Microsoft a rendu public un outil pour interpréter la majorité des mesures : **PCPTool**

https://github.com/Microsoft/TSS.MSR

# Attestation de santé

**Contrecarrer les attaques plus sophistiqués : détecter la compromission de l'hôte**

1. Relever la configuration de la machine
2. Durcir la politique d'exécution de codes

Durant l'amorçage :

1

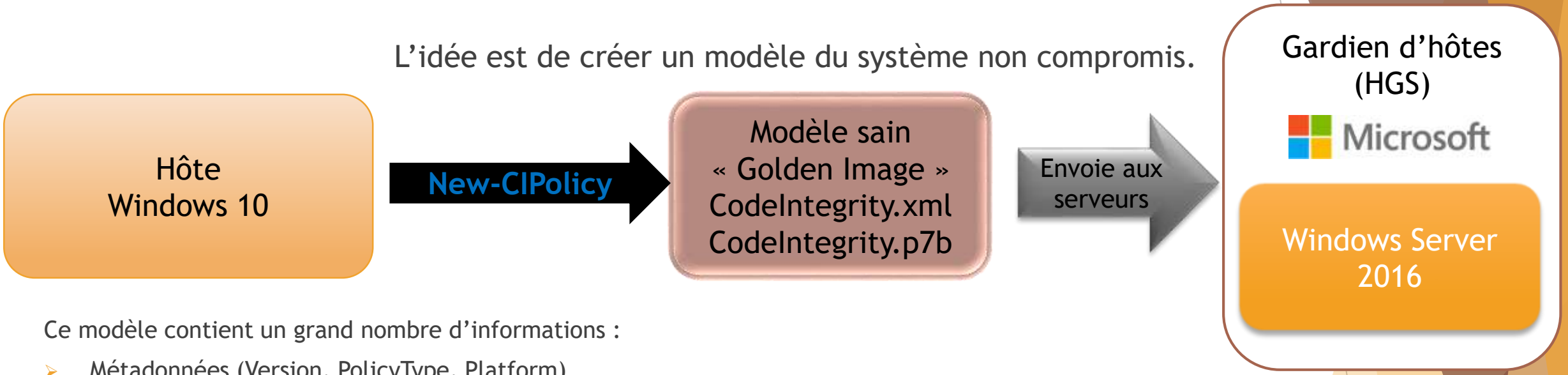
***Secure Boot*** est activé;

La puce **TPM** effectue des mesures fiables des instructions chargées lors de la chaîne de démarrage.

# Code Integrity Policy

**Effectuer une mesure des fichiers systèmes post-amorçage.**

L'idée est de créer un modèle du système non compromis.




Ce modèle contient un grand nombre d'informations :

- Métadonnées (Version, PolicyType, Platform)
- Jeux de règles
- Extended Key Usage (EKU)
- Règles sur les fichiers (Allow ID Name Hash MinimumFileVersion)
- Information sur les signataires des fichiers systèmes
- Information sur les signataires des drivers
- Politique de mise à jour
- Information sur les signataires de la politique d'intégrité du code
- L'utilisation de Hyper-V Code Integrity

# Attestation – TPM Trusted

**Permettre une protection des machines virtuelles en cas de compromissions de l'hôte.**

Hôte

Hyper-V

TPM

UEFI

Secure Boot

Code Integrity

Demande d'attestation + TPM EKPub

Nonce

Quote(Nonce, PCR(0-14), AIK) + Certificat AIK

Demande TCGLog

Gardien

Host Guardian Services


Mesures de références :

- TPM Endorsement Key
- TCGLog
- Code Integrity Policy

# Attestation – TPM Trusted

**Permettre une protection des machines virtuelles en cas de compromissions de l'hôte.**

Hôte

Hyper-V

TPM

UEFI

Secure Boot

Code Integrity

Demande d'attestation

Nonce

Quote(Nonce, PCR(0-14), AIK) + Certificat AIK

Demande TCGLog

TCGLog

UEFI CPR (*CPU Recall Parameter*) (DebugMode)
Virtual Secure Mode ID
Virtual Secure Mode Public Key (VSMIDK)
Hypervisor Code Integrity

Attestation de santé

Gardien

Host Guardian Services

Mesures de références :

- TPM Endorsement Key
- TCGLog
- Code Integrity Policy


Vérifie la validité du certificat AIK

Recalcule les empreintes et compare avec la quote

Compare le TCGLog avec la référence

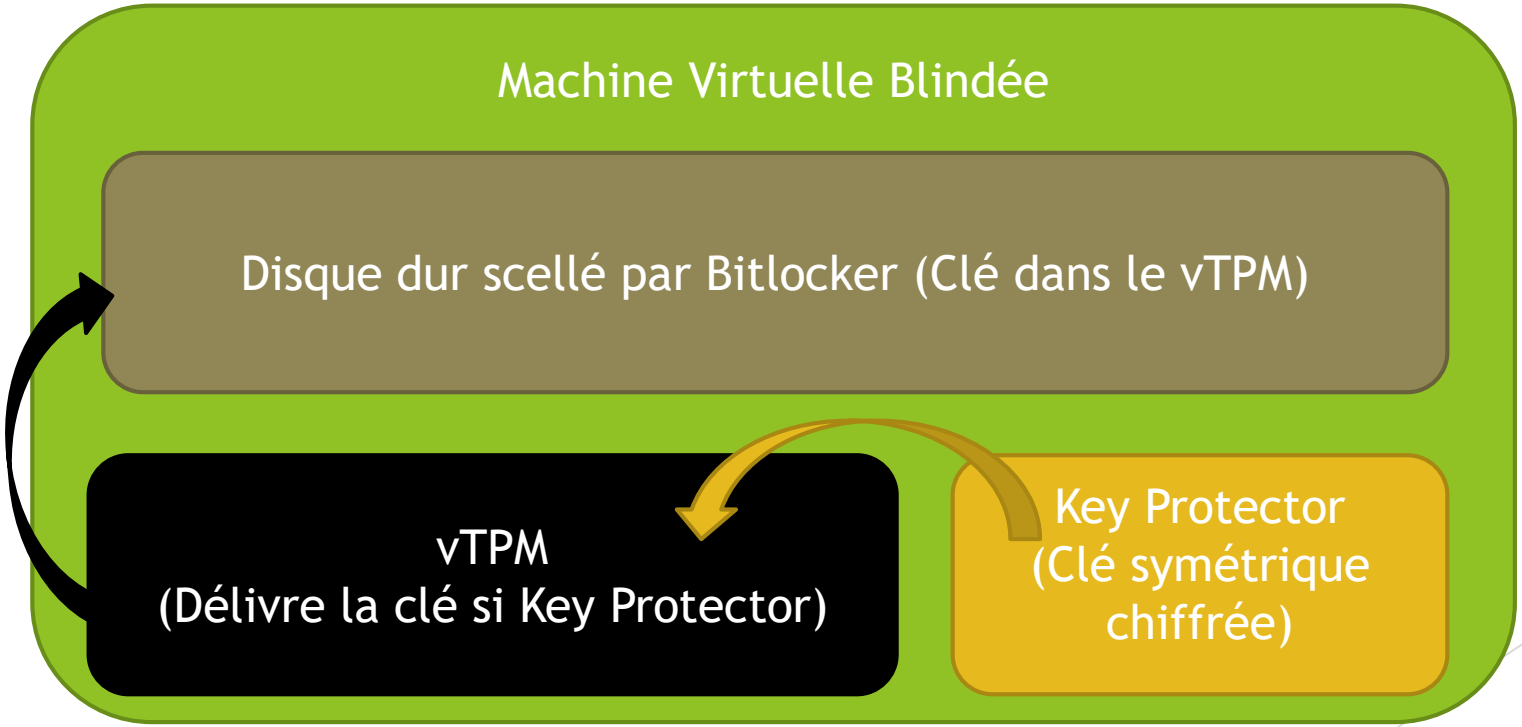
Déduit du TCGLog la clé publique VSMIDK

Création d'une attestation de santé (Certificat X.509)

# vTPM - Bitlocker

Durant le déploiement :

- Création d'une VM
- Ajout d'une ressource Key Protector
- Installation vTPM
- Installation Bitlocker



# Key Protector

**Partager un secret (clé de transport) entre plusieurs personnes dans un même fichier**

**Situation initiale**

# Key Protector

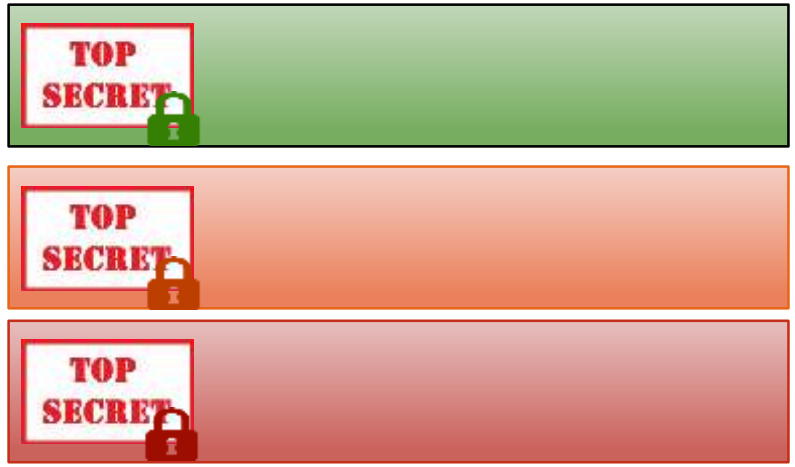
**Partager un secret (clé de transport) entre plusieurs personnes dans un même fichier**

**Situation initiale**

**Lors de la génération du secret :**

Secret généré


Fichier de sortie



# Key Protector

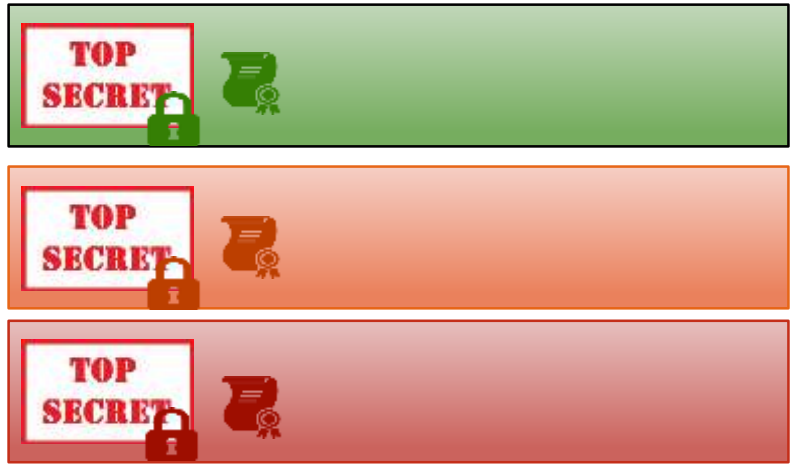
**Partager un secret (clé de transport) entre plusieurs personnes dans un même fichier**

**Situation initiale**

**Lors de la génération du secret :**

Secret généré


Fichier de sortie



# Key Protector

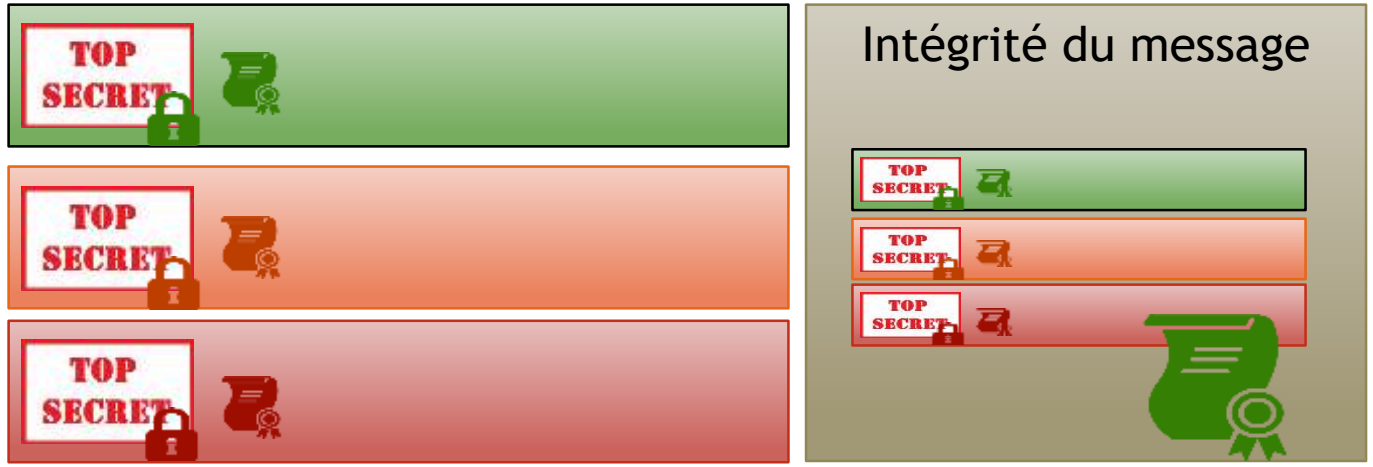
**Partager un secret (clé de transport) entre plusieurs personnes dans un même fichier**

**Situation initiale**

**Lors de la génération du secret :**

Secret généré


Fichier de sortie



# Key Protector

**Partager un secret (clé de transport) entre plusieurs personnes dans un même fichier**

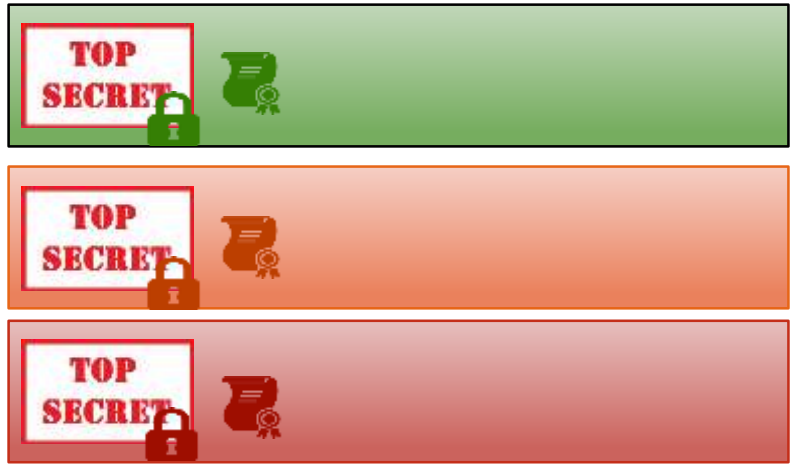
## Situation initiale

| Hôte | Gardien 1 | Gardien 2 |
|---|---|---|
| Certificats de signature et chiffrement | Certificats de signature et chiffrement | Certificats de signature et chiffrement |

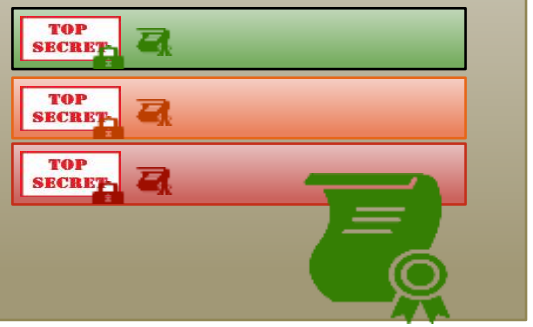
## Lors de la génération du secret :

Secret généré


Fichier de sortie




Intégrité du message



# Key Protector

**Partager un secret (clé de transport) entre plusieurs personnes dans un même fichier**

## Situation initiale

Hôte
Certificats de signature et chiffrement

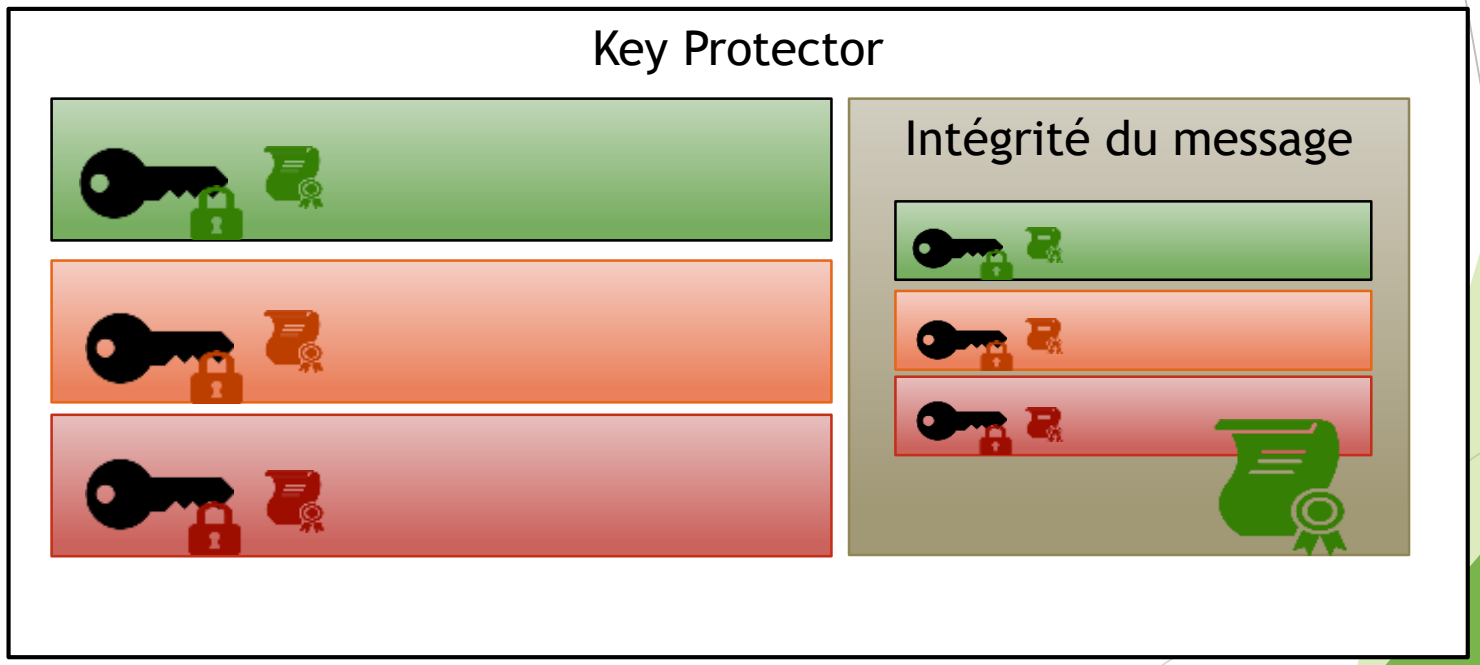
Gardien 1
Certificats de signature et chiffrement

Gardien 2
Certificats de signature et chiffrement

## Lors de la génération du secret :

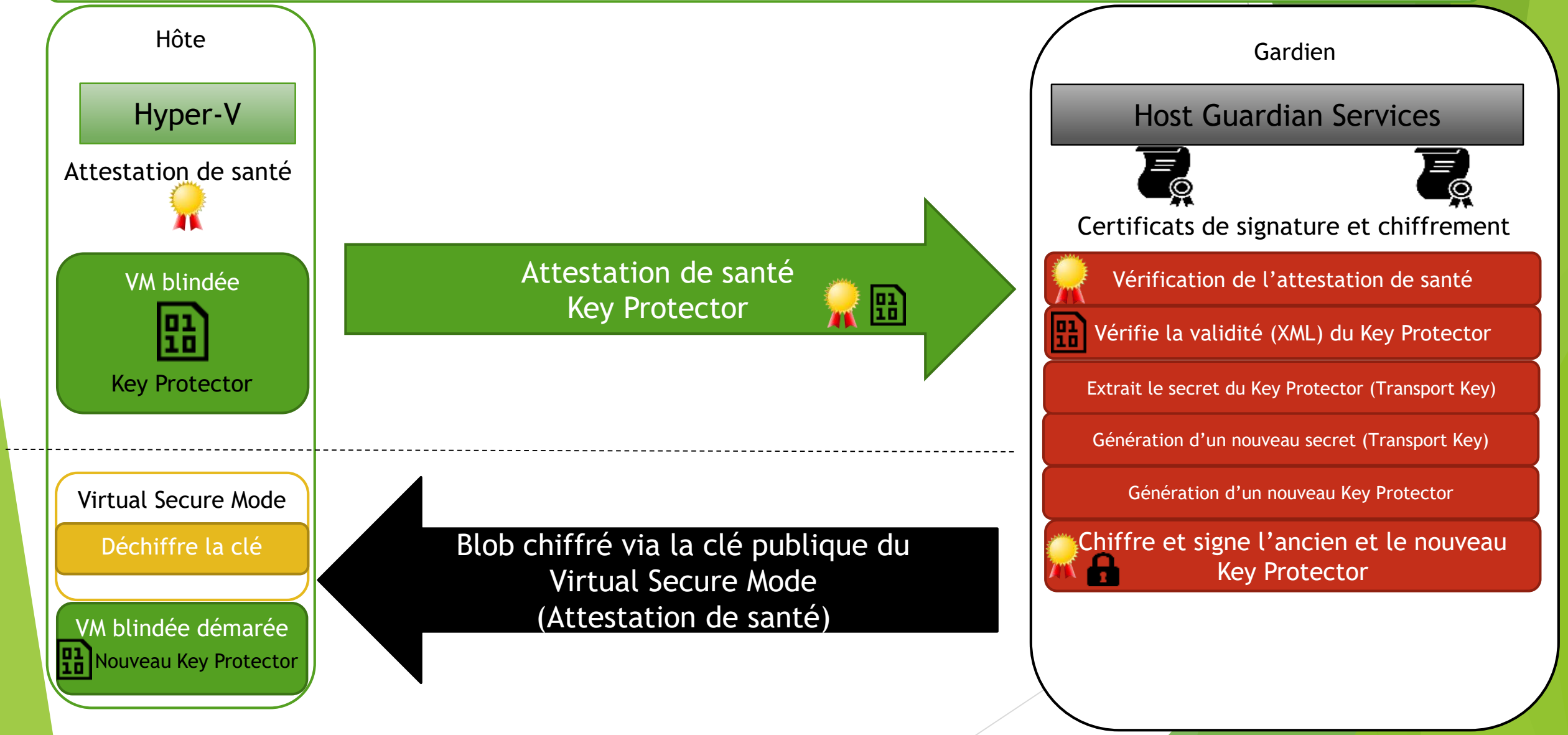
Secret généré

Clé de Transport



# Idée globale

**Permettre une protection des machines virtuelles en cas de compromissions de l'hôte.**



# Key Protection Services - Requête

Ingress protector (base64 – XML)

## Certificat de l'hôte

Certificat de signature :

- Pour : Hôte
- De : Hôte
- Validité : 10 ans
- Clé publique : RSA 2048

Certificat de chiffrement :

- Pour : Hôte
- De : Hôte
- Validité : 10 ans
- Clé publique : RSA 2048

Clé de transport chiffrée

Signatures des certificats

## Certificat des HGS

Certificat de signature :

- Pour : HGS
- De : CA
- Validité : 1 an
- Clé publique : RSA 2048

Certificat de chiffrement :

- Pour : HGS
- De : CA
- Validité : 1 an
- Clé publique : RSA 2048

Clé de transport chiffrée

Signatures des certificats

## Clé

Méthode de dérivation de clé SP800 108 CTR HMAC KDF

Signature de la clé de transport

Signature du garde + ID

## Certificat de santé (X509) :

- Pour : Authorized Host Identifier
- De : Microsoft Remote Attestation Service
- Validité : 8 heures
- Clé publique : RSA 2048

## Algorithme de chiffrement de clé :

- TransferKeyEncryptionAlgorithm RSA-OAEP-MGF1-SHA256
- TransportKeyEncryptionAlgorithm AES-GCM
- WrappingKeyEncryptionAlgorithm AES-GCM

Hôte → IP – TCP – HTTP(S) - XML → HGS

# Key Protection Services - Réponse

Egress Key protector (base64 – XML)

## Certificat de l'hôte

Certificat de signature :

- Pour : Hôte
- De : Hôte
- Validité : 10 ans
- Clé publique : RSA 2048

Certificat de chiffrement :

- Pour : Hôte
- De : Hôte
- Validité : 10 ans
- Clé publique : RSA 2048

Clé de transport chiffrée

Signatures des certificats

## Certificat des HGS

Certificat de signature :

- Pour : HGS
- De : CA
- Validité : 1 an
- Clé publique : RSA 2048

Certificat de chiffrement :

- Pour : HGS
- De : CA
- Validité : 1 an
- Clé publique : RSA 2048

Clé de transport chiffrée

Signatures des certificats

## Clé

Méthode de dérivation de clé SP800 108 CTR HMAC KDF

Signature de la clé de transport

Signature du garde + ID

Clés :

- Encrypted Transfer Key RSA-OAEP-MGF1-SHA256
- Encrypted Wrapping Key AES-GCM
- Encrypted Transport Key AES-GCM

HGS → IP – TCP – HTTP(S) - XML → Hôte


# Réception des clés - Trustlets

VTL 0

Virtual Machine Worker Process
vmwp.exe (PPL)

wmiprvse.exe

VTL 1

Virtual Machine Security Process
vmsp.exe

vTPM Trustlet

Autorise Event Tracing for Windows
Interdit Debugger
Désactive Crash Dump

vTPM Key Enrollment Trustlet

# Et maintenant ?

- Etudier le mécanisme de réception des clés
- Etudier l'interaction entre le VMWP et VMSP