# BitLocker

Aurélien Bordes – aurelien26@free.fr

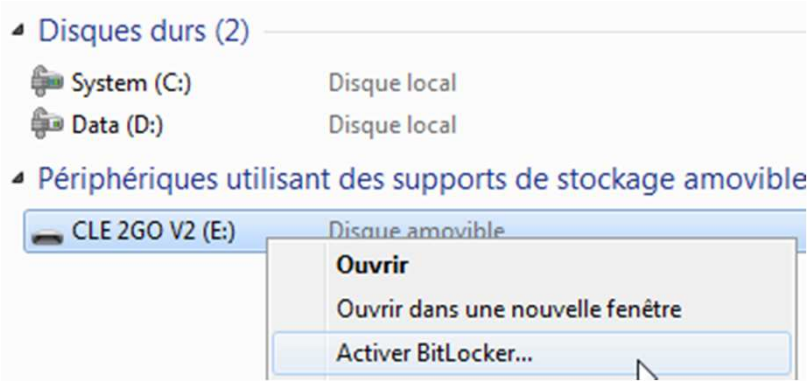
SSTIC 2011

8 juin 2011

# BitLocker rapidement

- Technologie apparue avec Windows Vista (éditions Entreprise et Intégrale) afin de répondre à un besoin important (confidentialité des données)
- Permet le chiffrement intégral du volume du système d'exploitation et de volumes de données
- Est totalement intégré et transparent pour les applications ou l'utilisateur
- Peut mettre en œuvre un module TPM afin de vérifier au démarrage l'intégrité du système

# Pourquoi étudier BitLocker ?





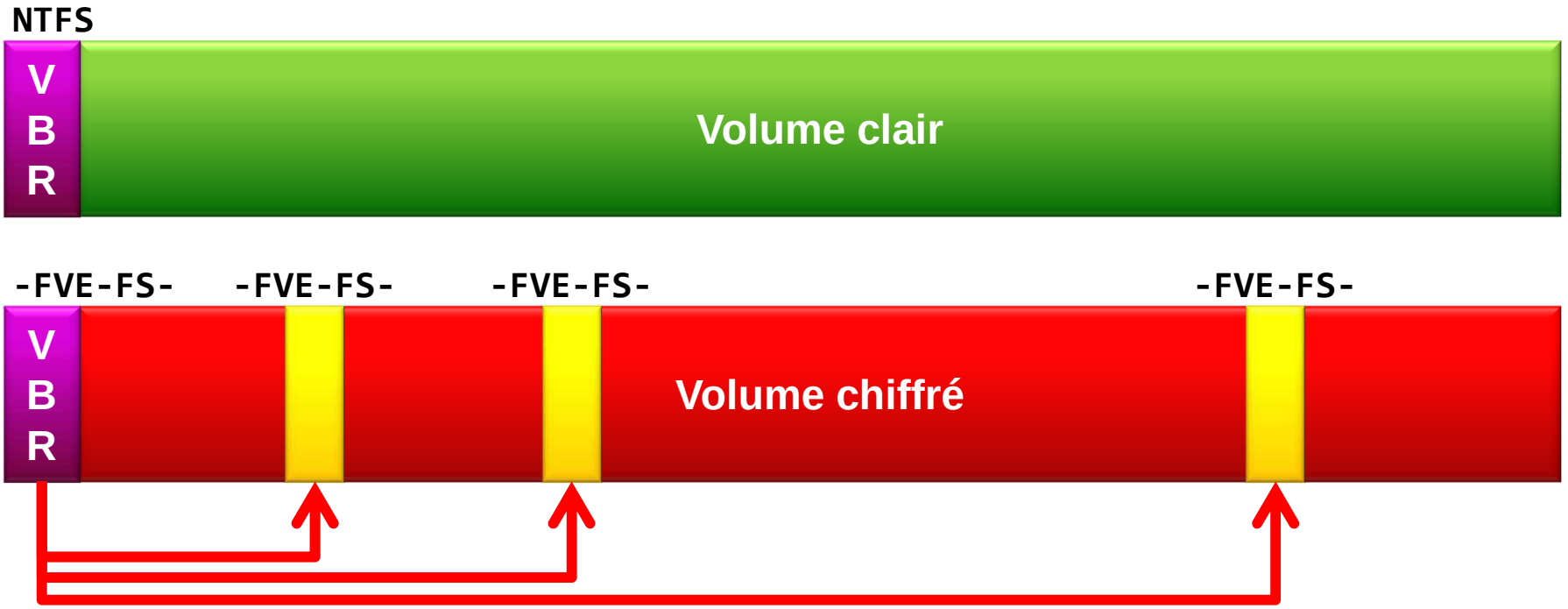
- Met en œuvre diverses technologies (*filter driver*, TPM, WMI, cryptographie, …)
- Ressort régulièrement dans l'actualité :
  - Fraunhofer Institute for Secure Information Technology : « *Attacking the BitLocker Boot Process* »
  - Christopher Tarnovsky, Black Hat 2010 : « *defeat the Trusted Platform Module* »
- Étudier les nouveautés de Windows 7

# Chiffrement & composants

# Contexte d'utilisation


- Partition de démarrage :
  - `bootmgr`, `BCD`, `memtest.exe`
- Partition système :
  - `Windows`, `Program Files` et `Users`

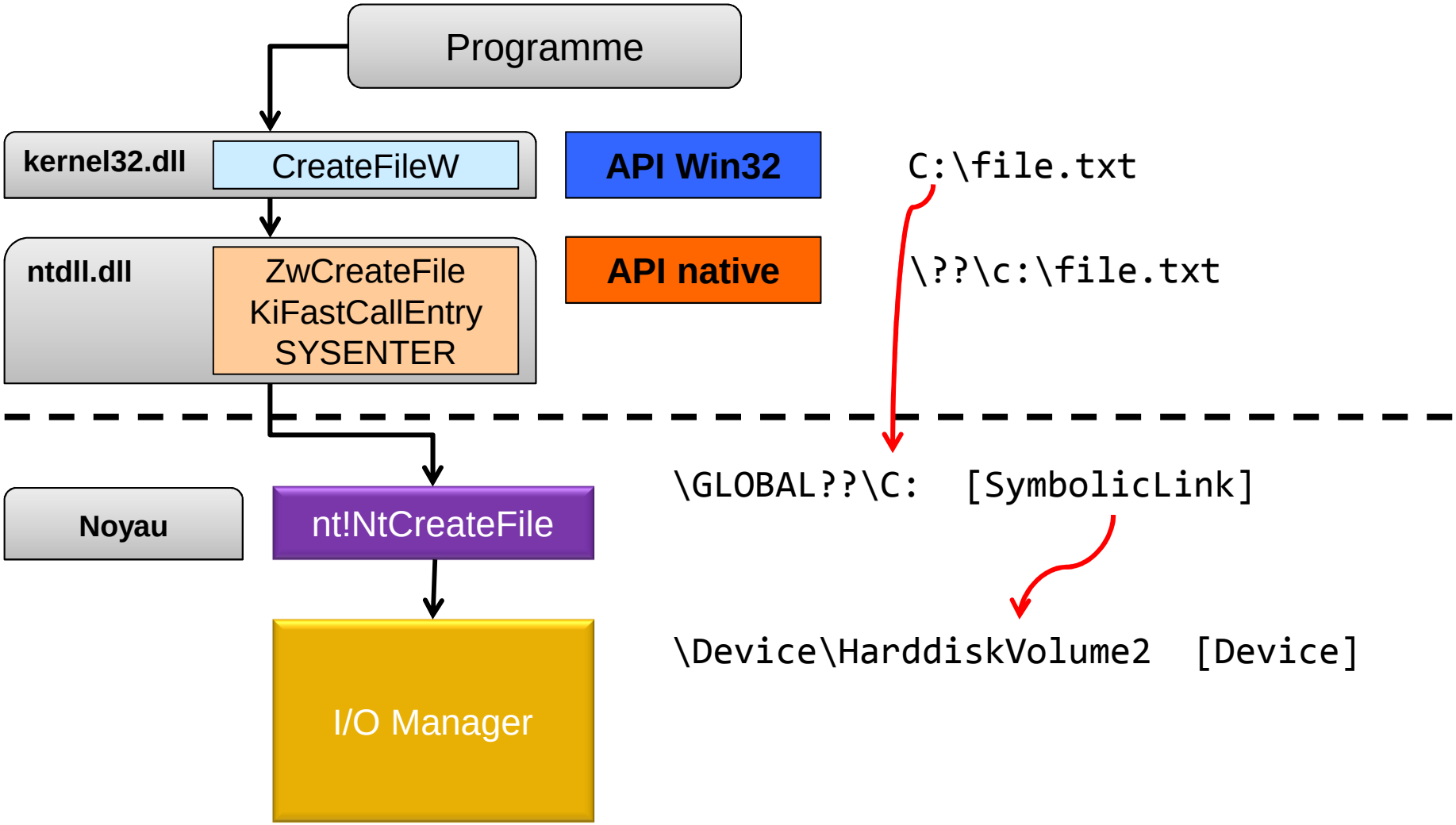
# Chiffrement d’un volume



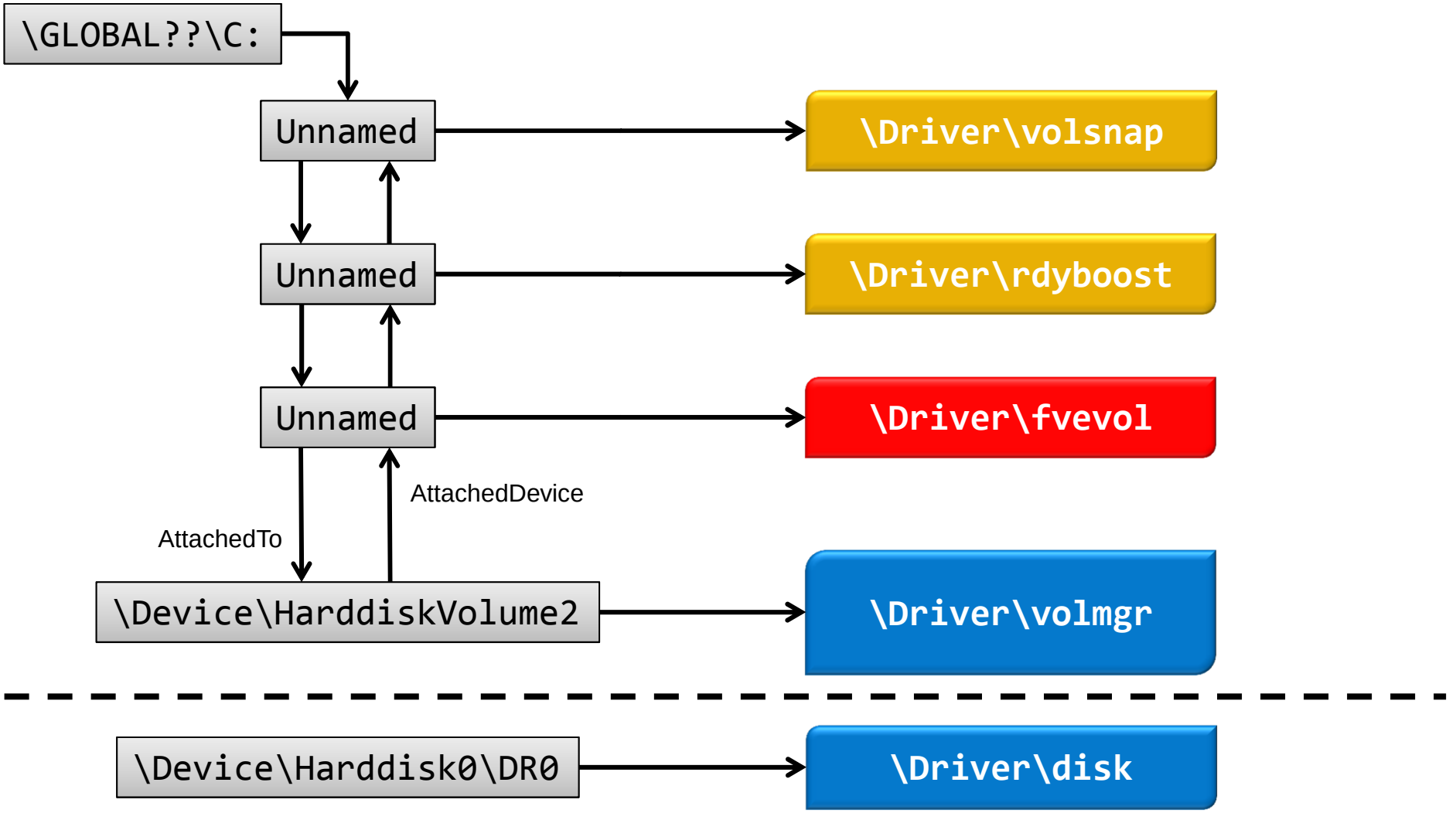

- L’intégralité du volume est chiffrée, à l’exception :
  - du Volume Boot Record (VBR)
  - de 3 zones de métadonnées

**FVE-FS : Full Volume Encryption File System**

# Intégration au système



# Liaison des périphériques

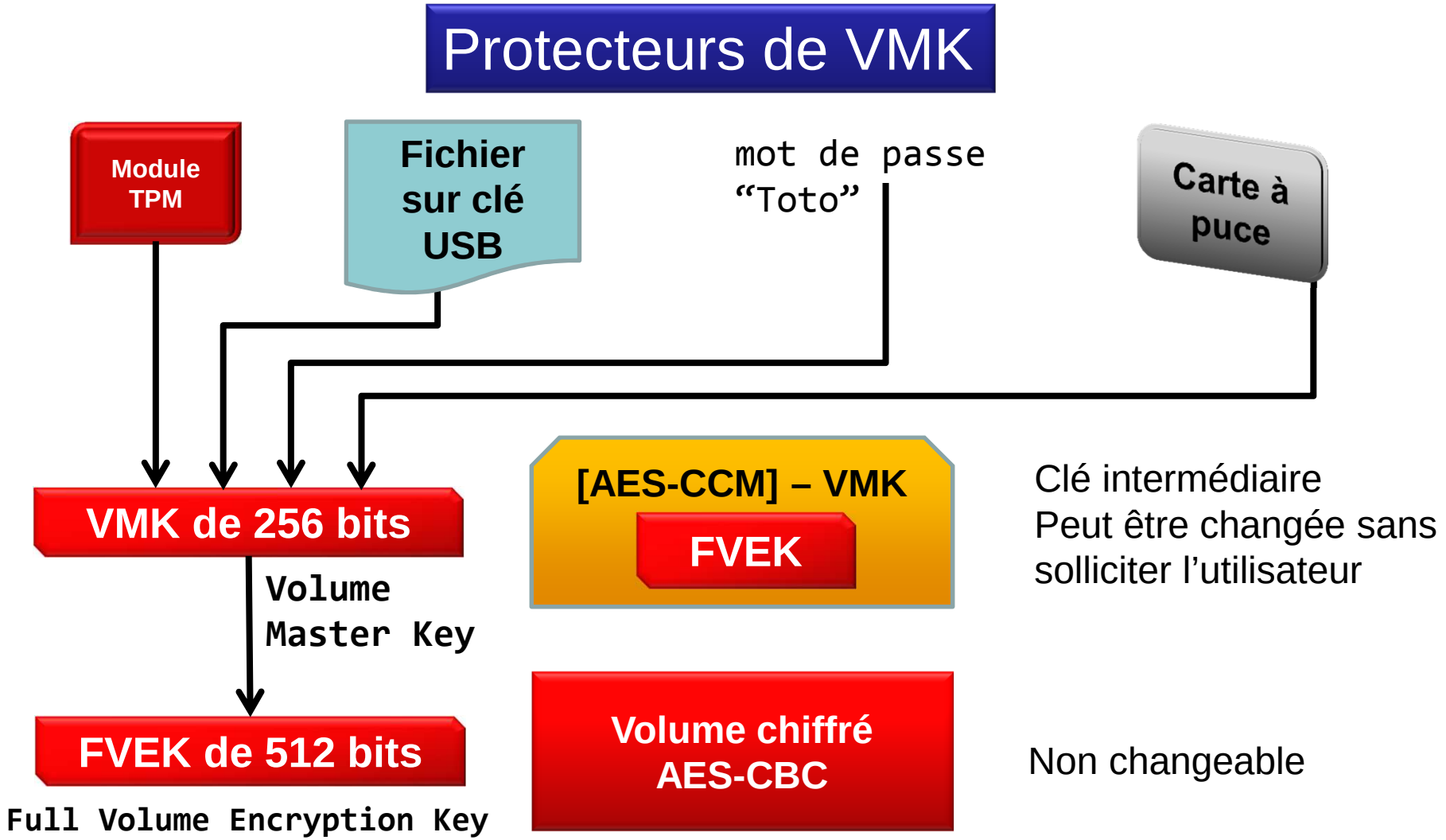


# Protecteurs VMK

# Chiffrement AES

- Deux modes d'AES sont mis en œuvre par BitLocker :
  - **AES-CBC** (*Cipher Block Chaining*) (avec ou sans diffuseur) pour le chiffrement du disque (clés de 128 ou 256 bits)
  - **AES-CCM** (*Counter with CBC-MAC*) pour le chiffrement des métadonnées de BitLocker (toujours clés de 256 bits)
    - Le mode CCM permet d'apporter un contrôle d'intégrité en plus du chiffrement

# Chaîne des clés



# Protecteurs VMK

- Il existe un protecteur VMK par type de protection mis en œuvre pour chaque volume qui permet :
  - le chiffrement de la VMK du volume (**Protection directe**)
  - l'obtention des éléments nécessaires à la régénération du protecteur en cas de changement de la VMK (**Protection inverse**)
  - l'exportation du mot de passe numérique ou de la clé externe (**Sauvegarde**)

# Protecteurs

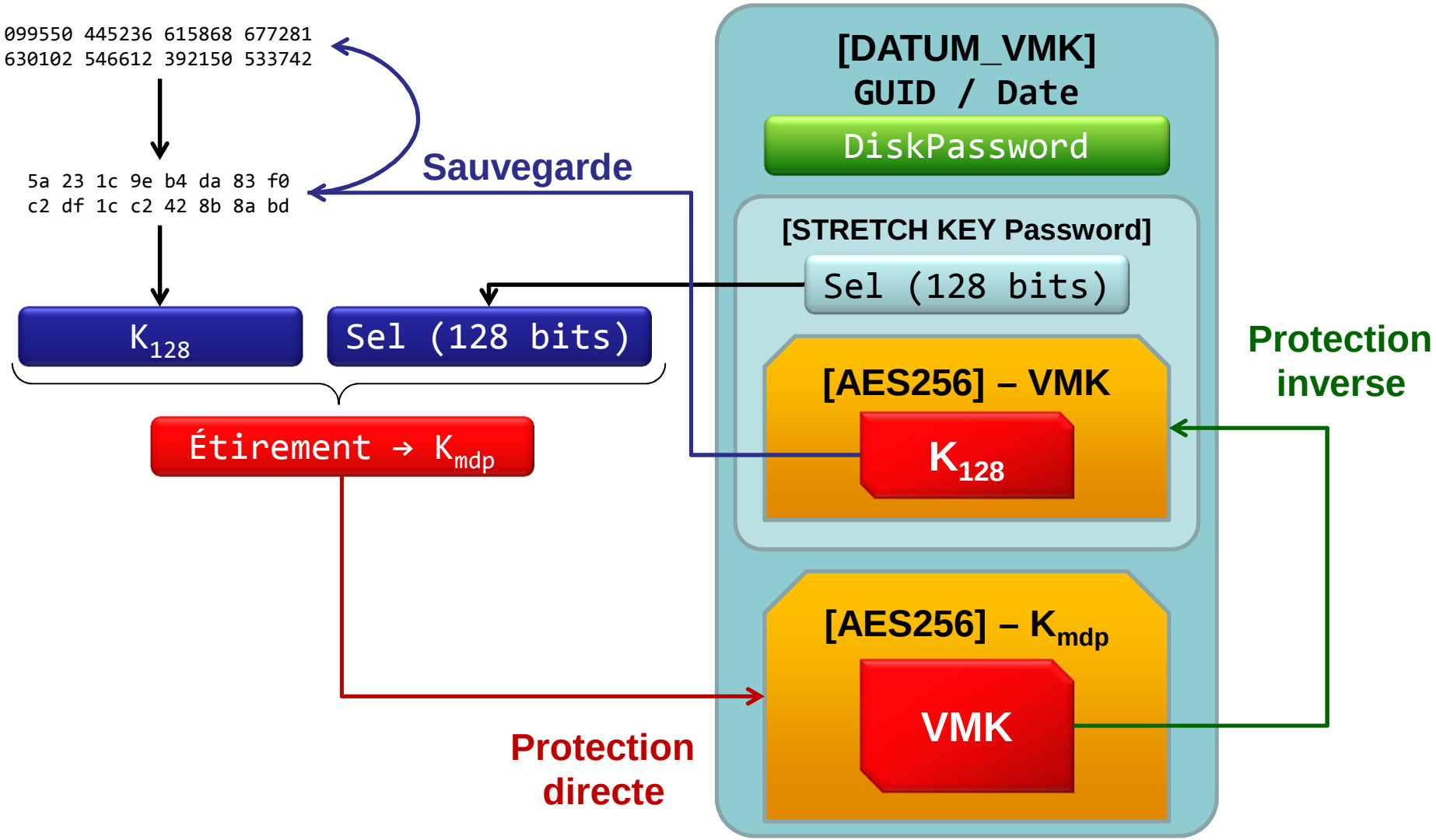
| ID WMI | Nom | Système | Données | Intégrité démarrage | Récupé-ration[x] |
|---|---|---|---|---|---|
| **3** | **Numerical password** | OUI | OUI | NON | OUI |
| 8 | Passphrase | NON | OUI | NON | OUI |
| 2 | External key | OUI | OUI | NON | OUI |
| 7 | Public Key | OUI | OUI | NON | OUI |
| 1 | TPM | OUI | NON | OUI | NON |
| **4** | **TPM And PIN** | OUI | NON | OUI | NON |
| 5 | TPM And Startup Key | OUI | NON | OUI | NON |
| 6 | TPM And PIN And Startup Key | OUI | NON | OUI | NON |

(x) mode de récupération en cas d'impossibilité d'obtenir la VMK par le TPM

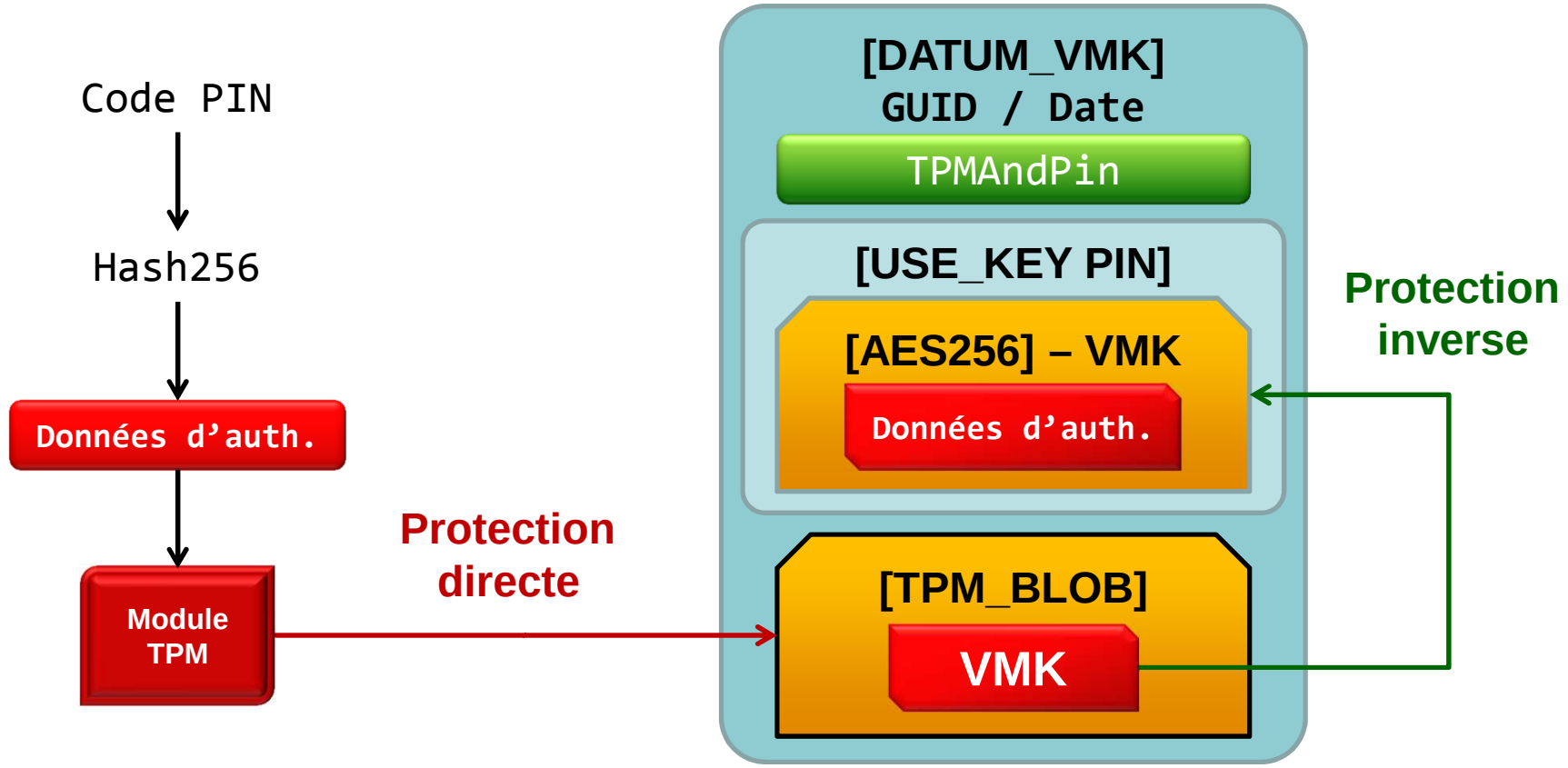
**Avec l'utilisation du TPM, un protecteur de récupération est recommandé**

# Mot de passe numérique

## (Numerical password, Recovery password)



# TPMAndPIN

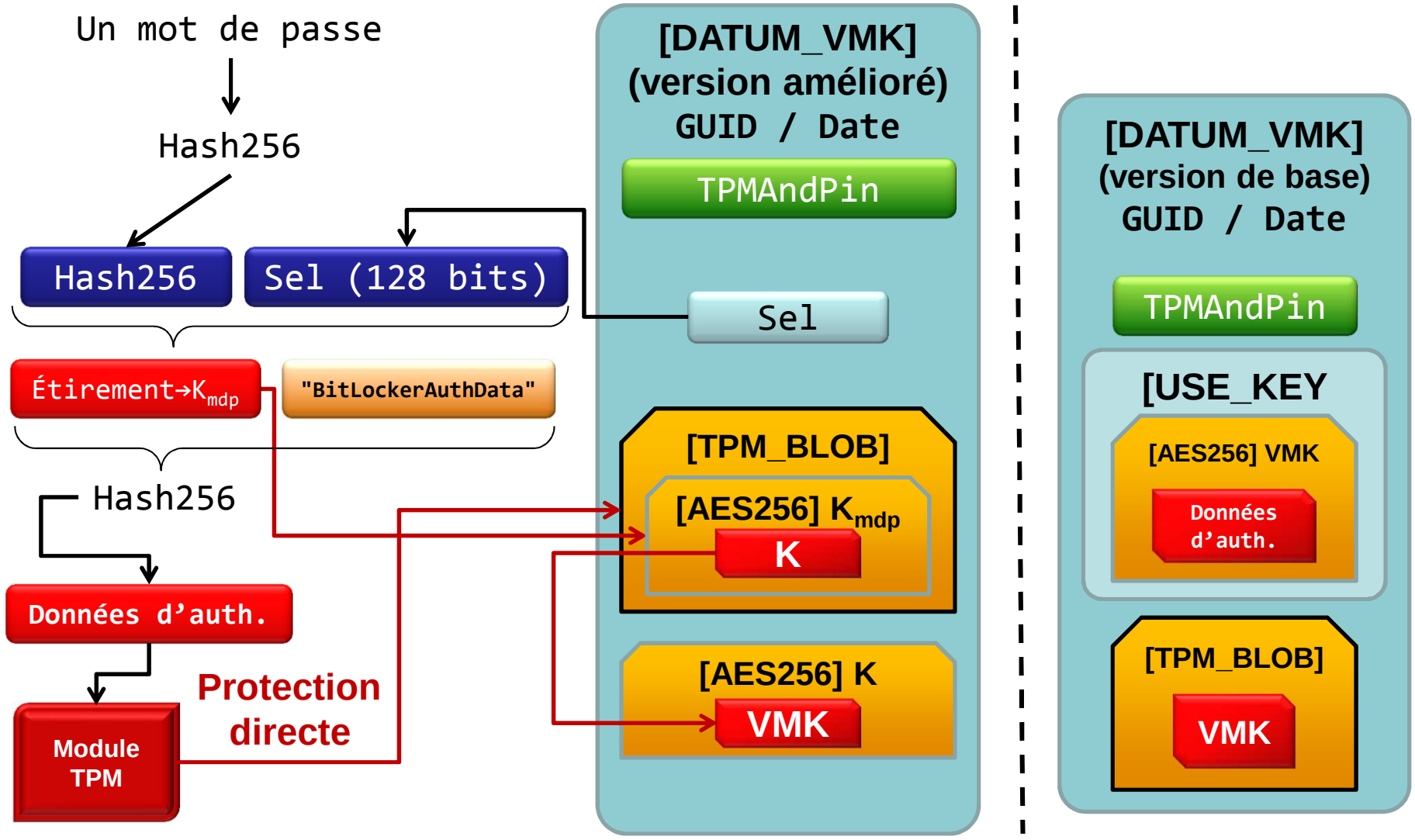

Code PIN
Hash256
Données d'auth.
Module TPM
Protection directe
[DATUM_VMK]
GUID / Date
TPMAndPin
[USE_KEY PIN]
[AES256] – VMK
Données d'auth.
[TPM_BLOB]
VMK
Protection inverse

# Améliorations Windows 7

- Problème d'attaque physique sur le TPM permettant de récupérer les clés privées du TPM donc de déchiffrer les TPM_BLOB (donc la VMK)
- Attaque impactant les modes **`TPM`** et **`TPMAndPIN`**
- Améliorations (« code confidentiel amélioré ») :
  - La VMK n'est plus protégée directement par le TPM mais par une clé intermédiaire
  - Après étirement, le code PIN (avec alphabet amélioré) est utilisé comme clé de chiffrement intermédiaire

# TPMAndPIN

## Version code PIN amélioré

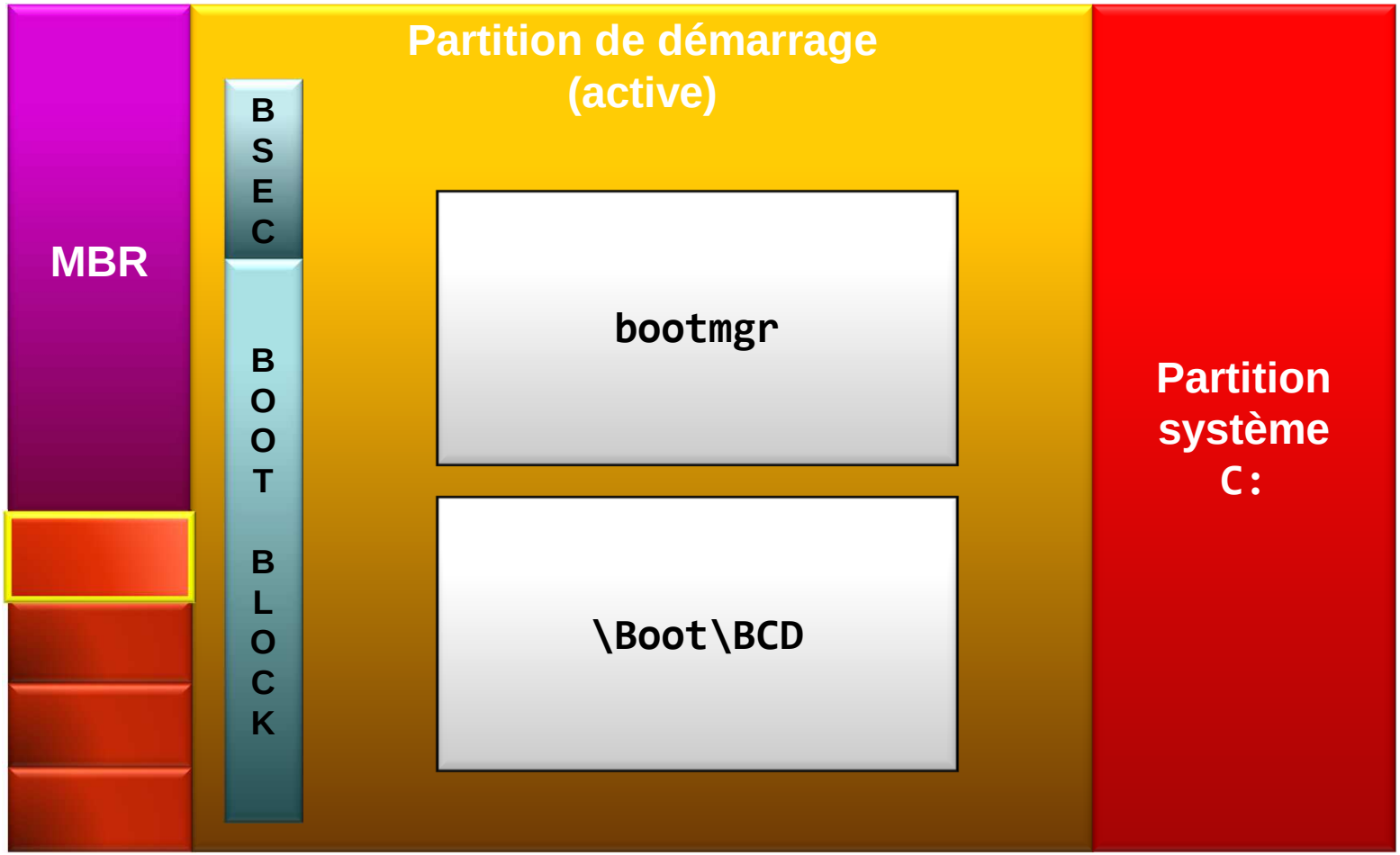


# Certificats

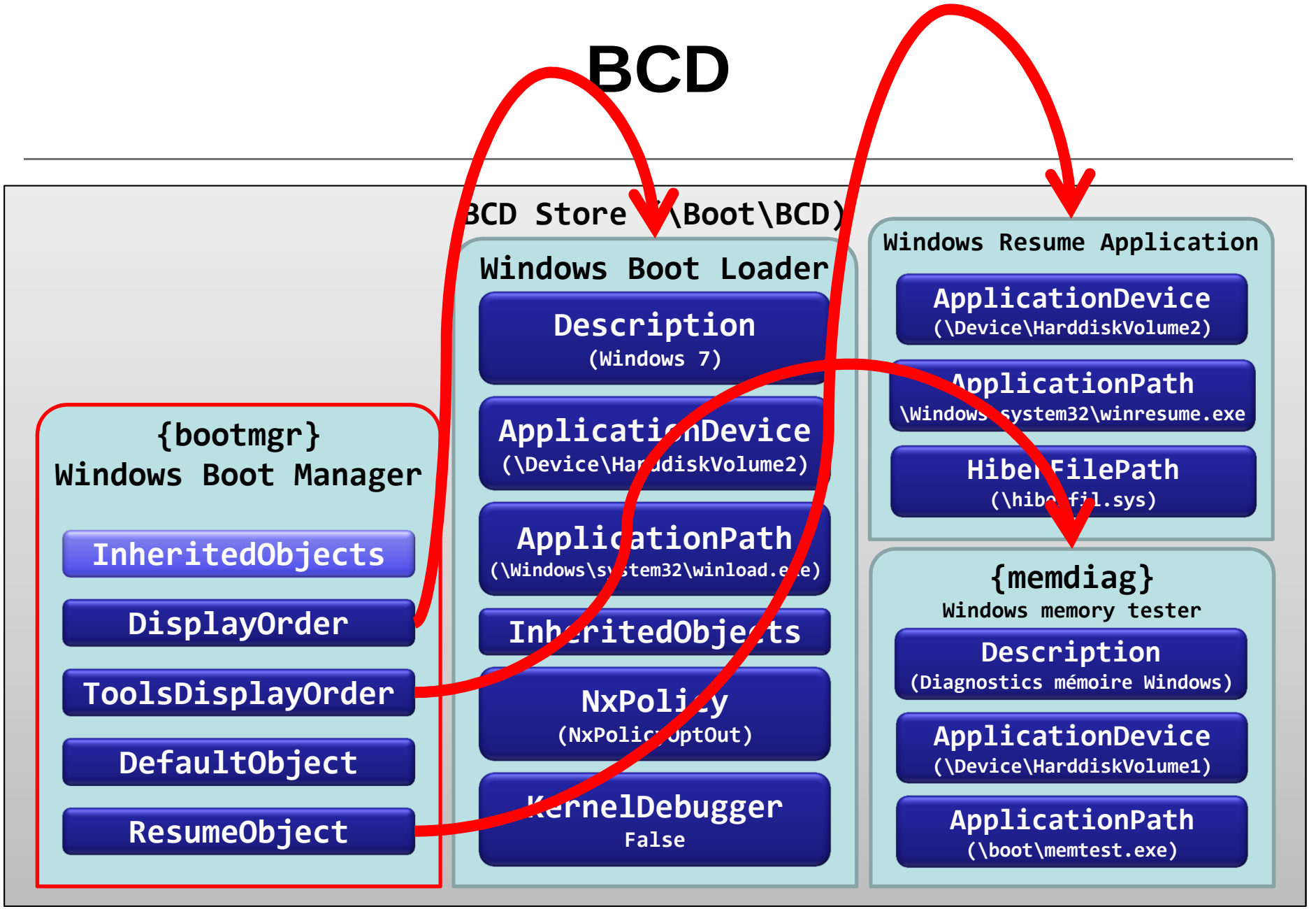
- Type de protecteur apparu avec Windows 7
- Permet l'utilisation d'une clé privée pour déchiffrer la VMK
- Méthode permettant :
  - L'utilisation d'une carte à puce
  - La récupération par certificat numérique
- Non utilisable pour démarrer un volume système

# Démarrage & mesures d’un système

# Démarrage (2)


MBR
BSEC
BOOT BLOCK
Partition de démarrage (active)
bootmgr
\Boot\BCD
Partition système C:

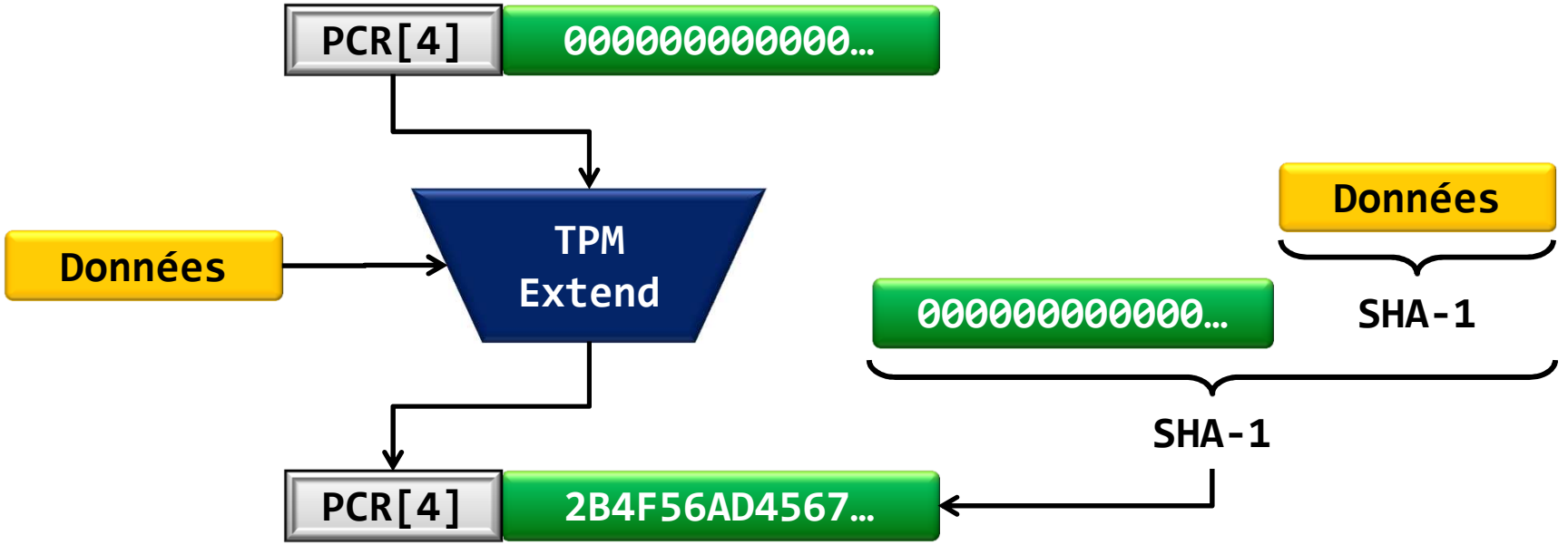
# BCD


{bootmgr}
Windows Boot Manager
InheritedObjects
DisplayOrder
ToolsDisplayOrder
DefaultObject
ResumeObject
BCD Store (\Boot\BCD)
Windows Boot Loader
Description
(Windows 7)
ApplicationDevice
(\Device\HarddiskVolume2)
ApplicationPath
(\Windows\system32\winload.exe)
InheritedObjects
NxPolicy
(NxPolicyOptOut)
KernelDebugger
False
Windows Resume Application
ApplicationDevice
(\Device\HarddiskVolume2)
ApplicationPath
\Windows\system32\winresume.exe
HiberFilePath
(\hiberfil.sys)
{memdiag}
Windows memory tester
Description
(Diagnostics mémoire Windows)
ApplicationDevice
(\Device\HarddiskVolume1)
ApplicationPath
(\boot\memtest.exe)

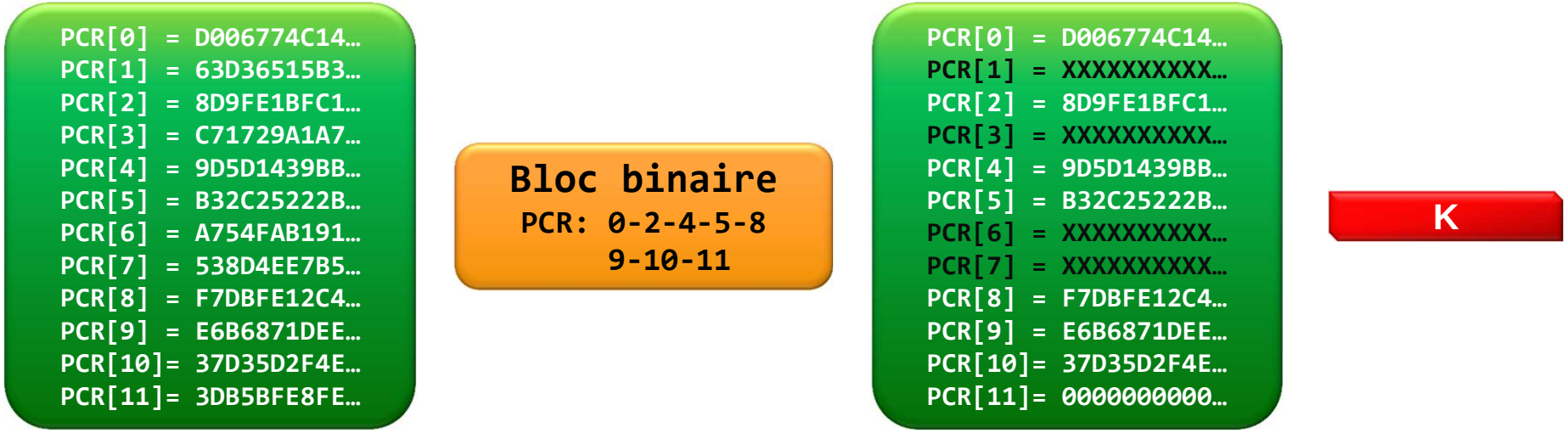
# Mesures du TPM via les PCR

- Les résultats des mesures sont étendues dans les registres PCR du TPM

$$PCR_{n+1} = SHA\text{-}1(PCR_n \mid SHA\text{-}1(Données))$$

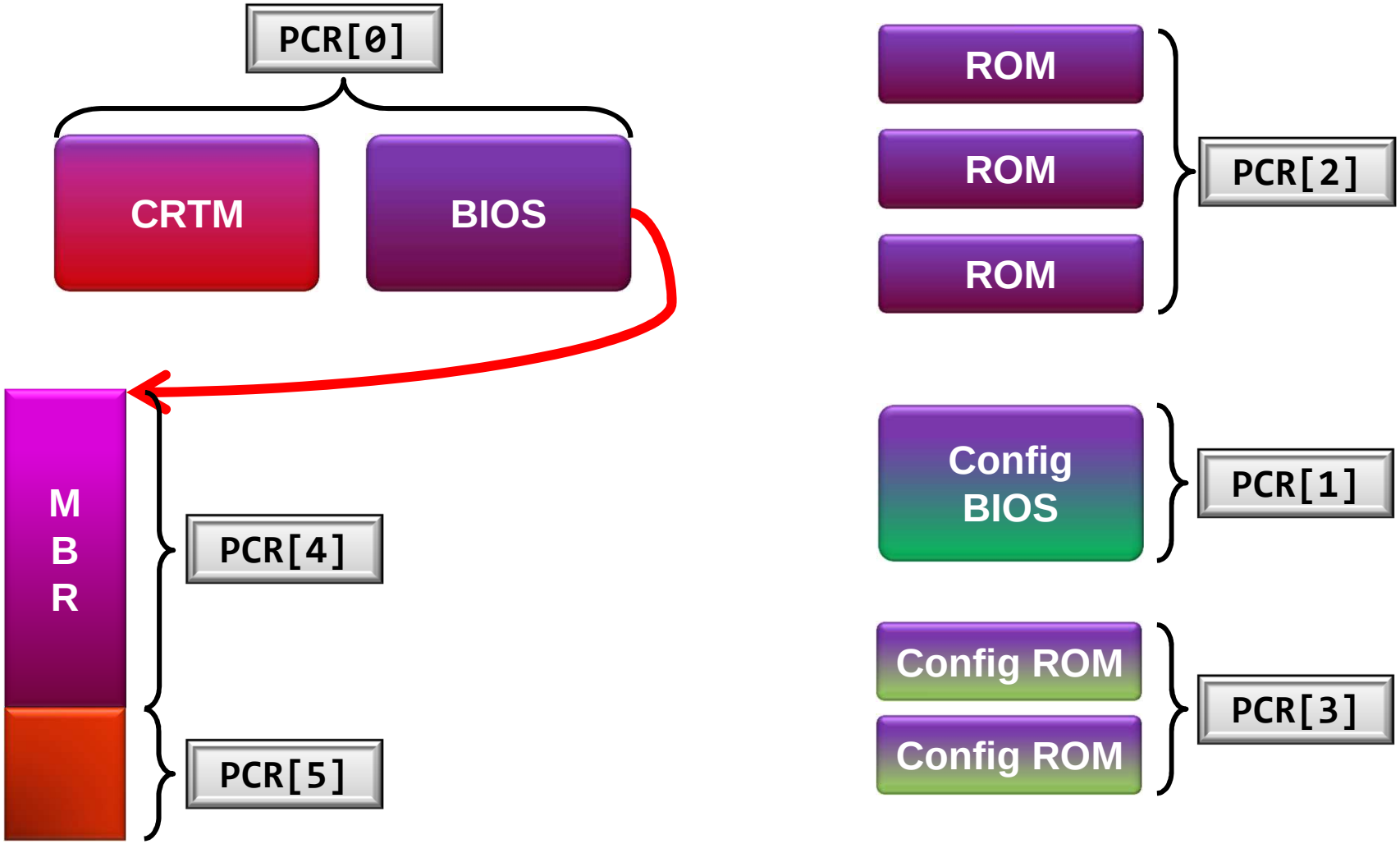


# Scellement et descellement par le TPM

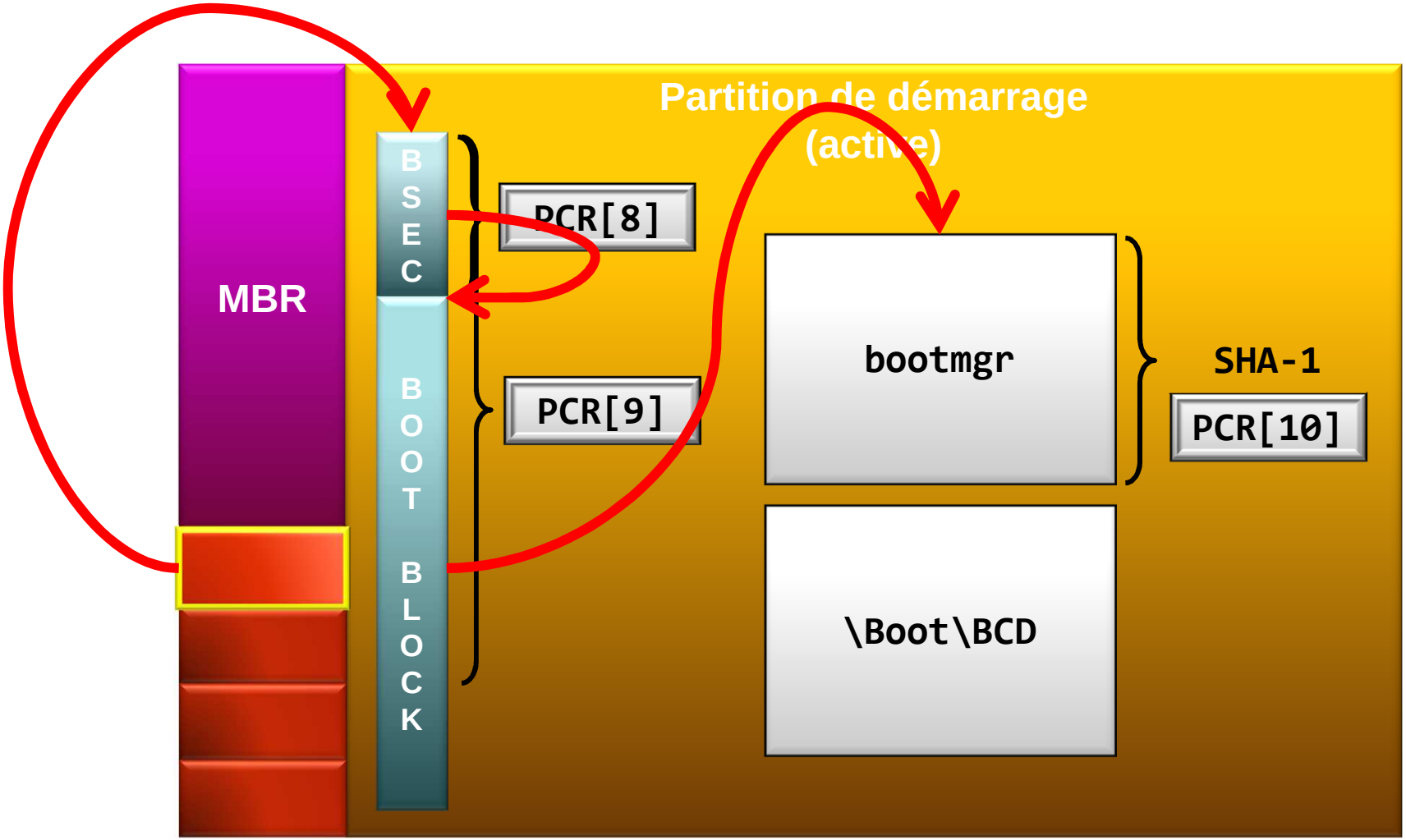



- Scellement par le TPM dans le cadre de BitLocker :
  - PCR sélectionnés : ceux du profil de validation (GPO)
  - Valeurs des PCR scellées : courantes (sauf PCR[11])
- Descellement :
  - Nécessite que les valeurs des PCR soient identiques à celles scellées dans le bloc

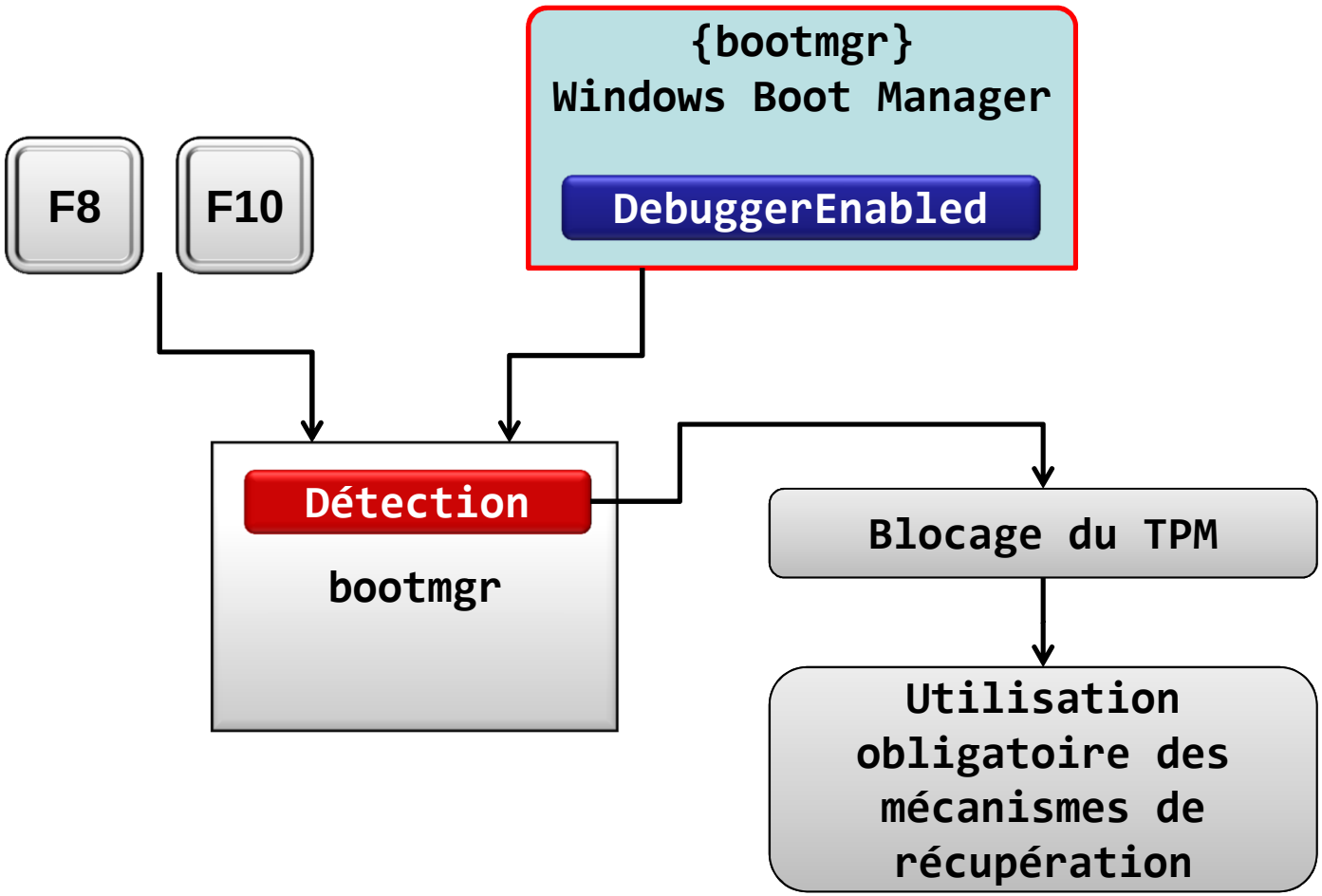
# Mesure des éléments du système
## Norme TCG (*Trusted Computing Group*)



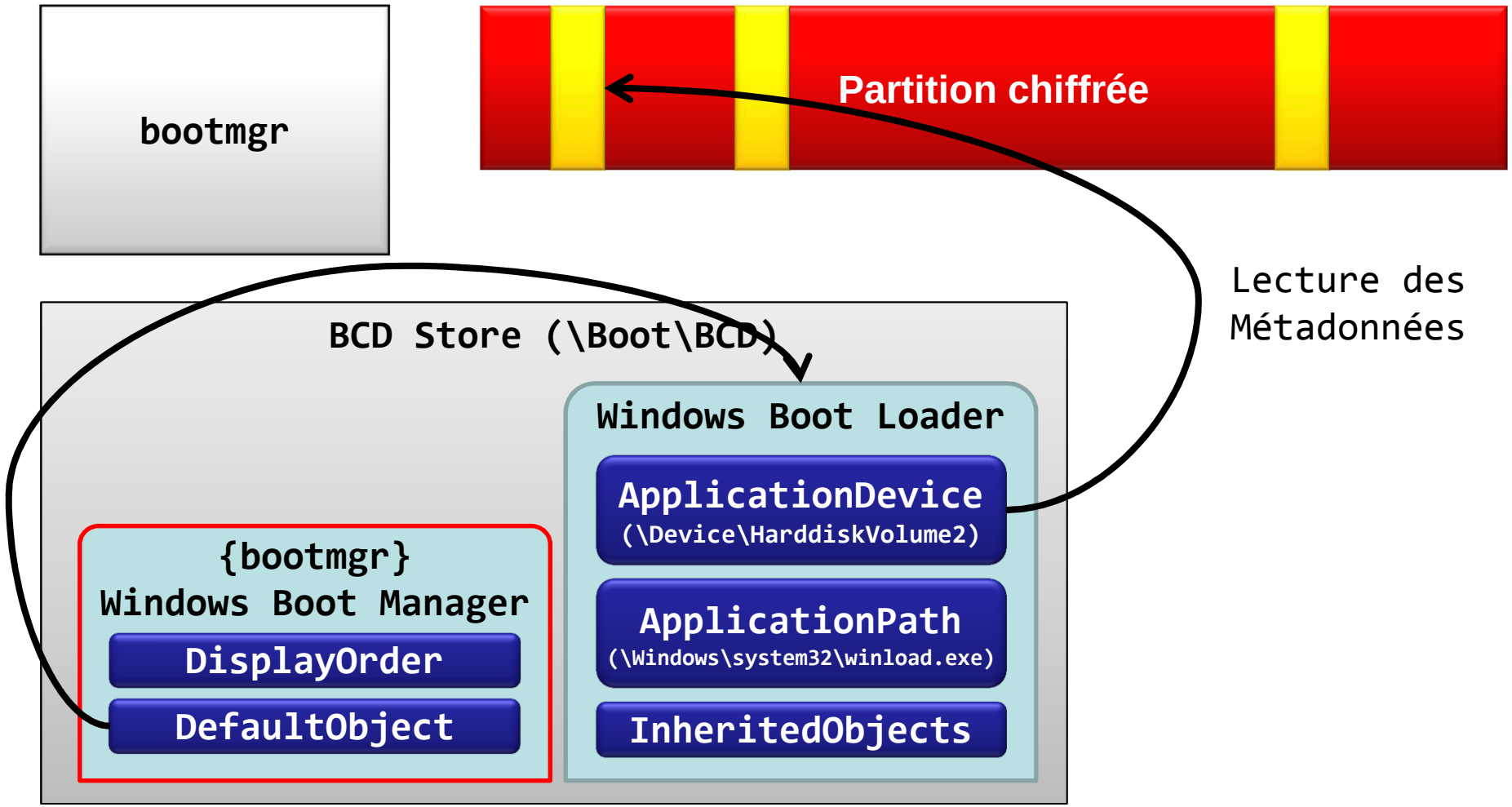
# Suite des mesures Spécifique Windows



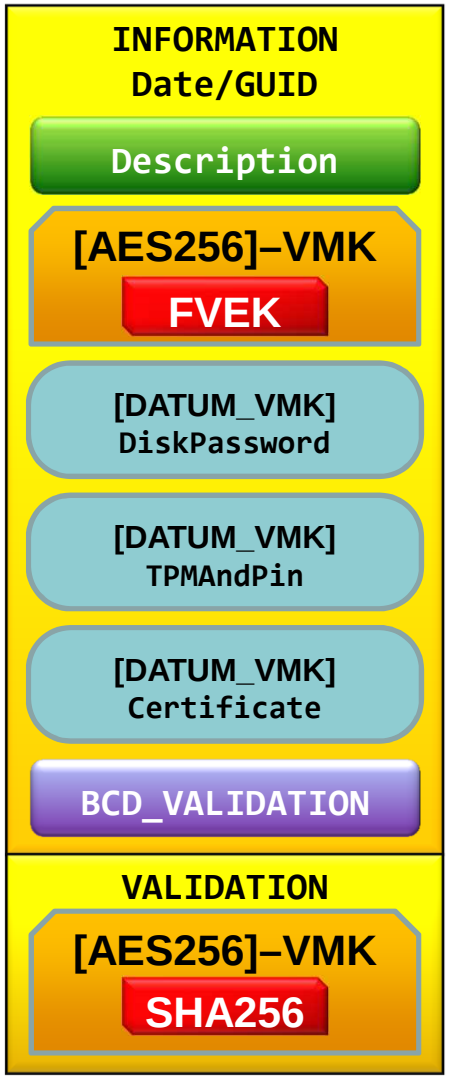
# Protections de *bootmgr*



# Suite du chargement



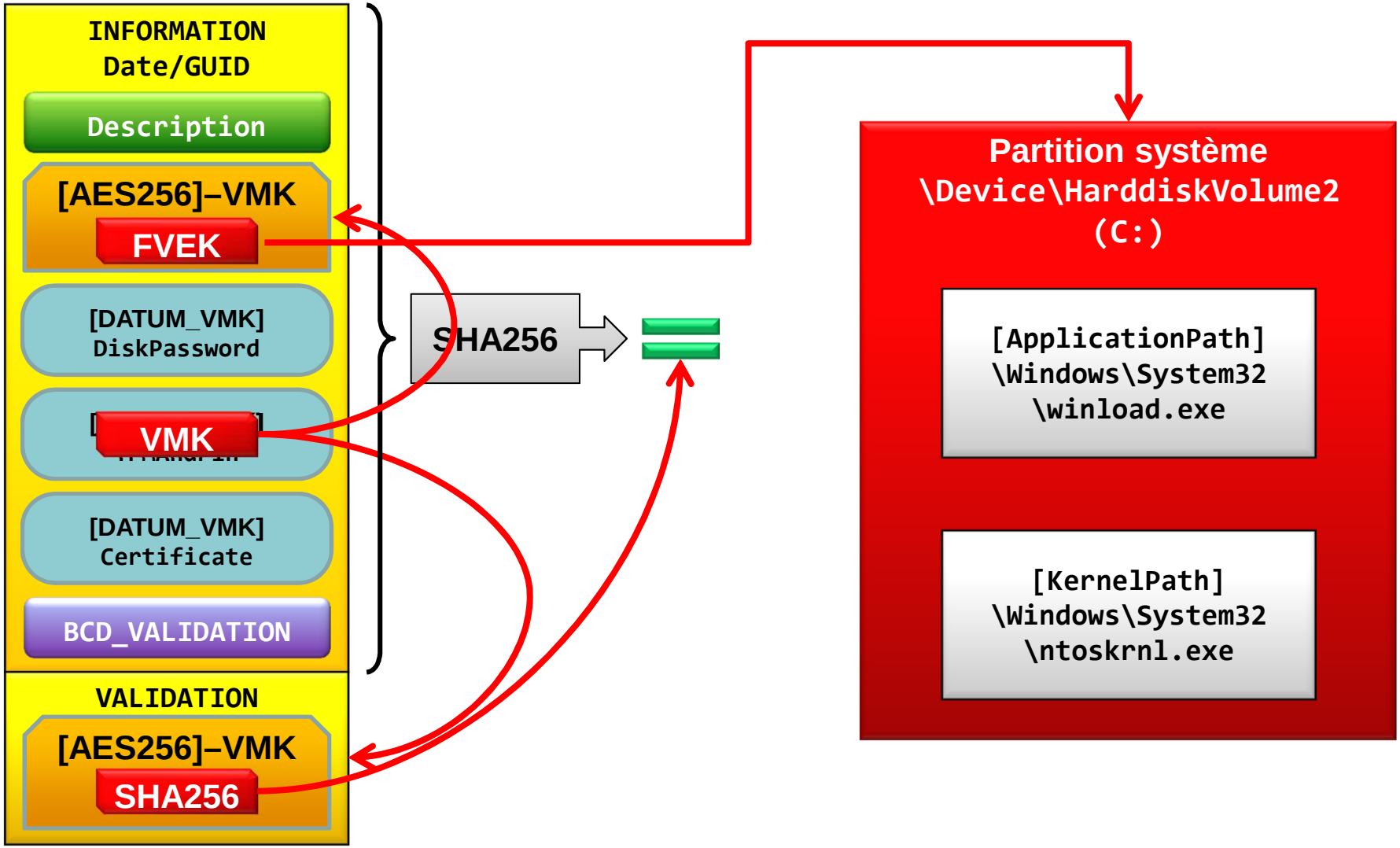
# Traitement des métadonnées



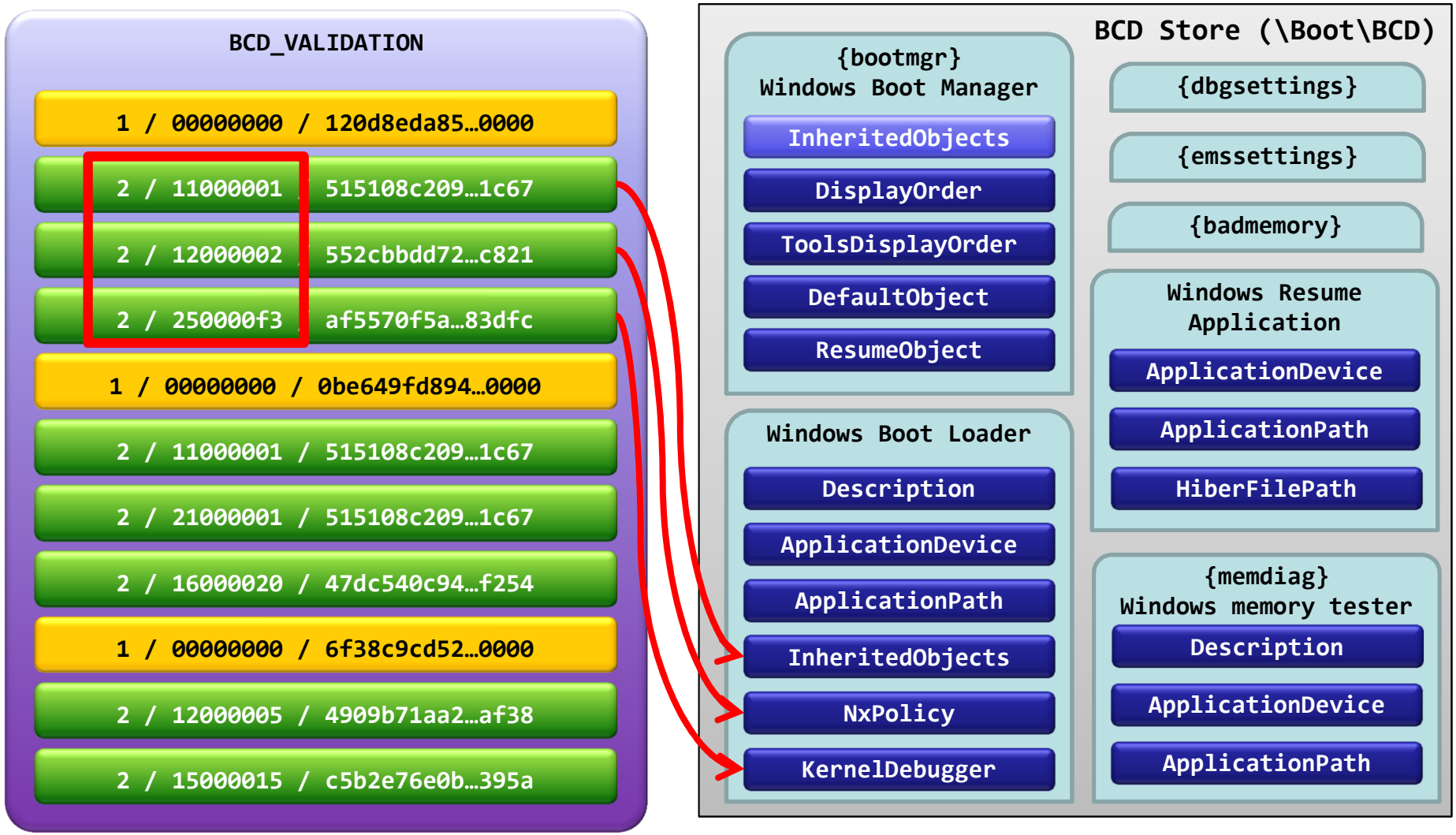

**Métadonnées**

- Priorité dans le choix des protecteurs :
  - D'abord ceux basés sur le TPM
  - Puis les autres (récupération)

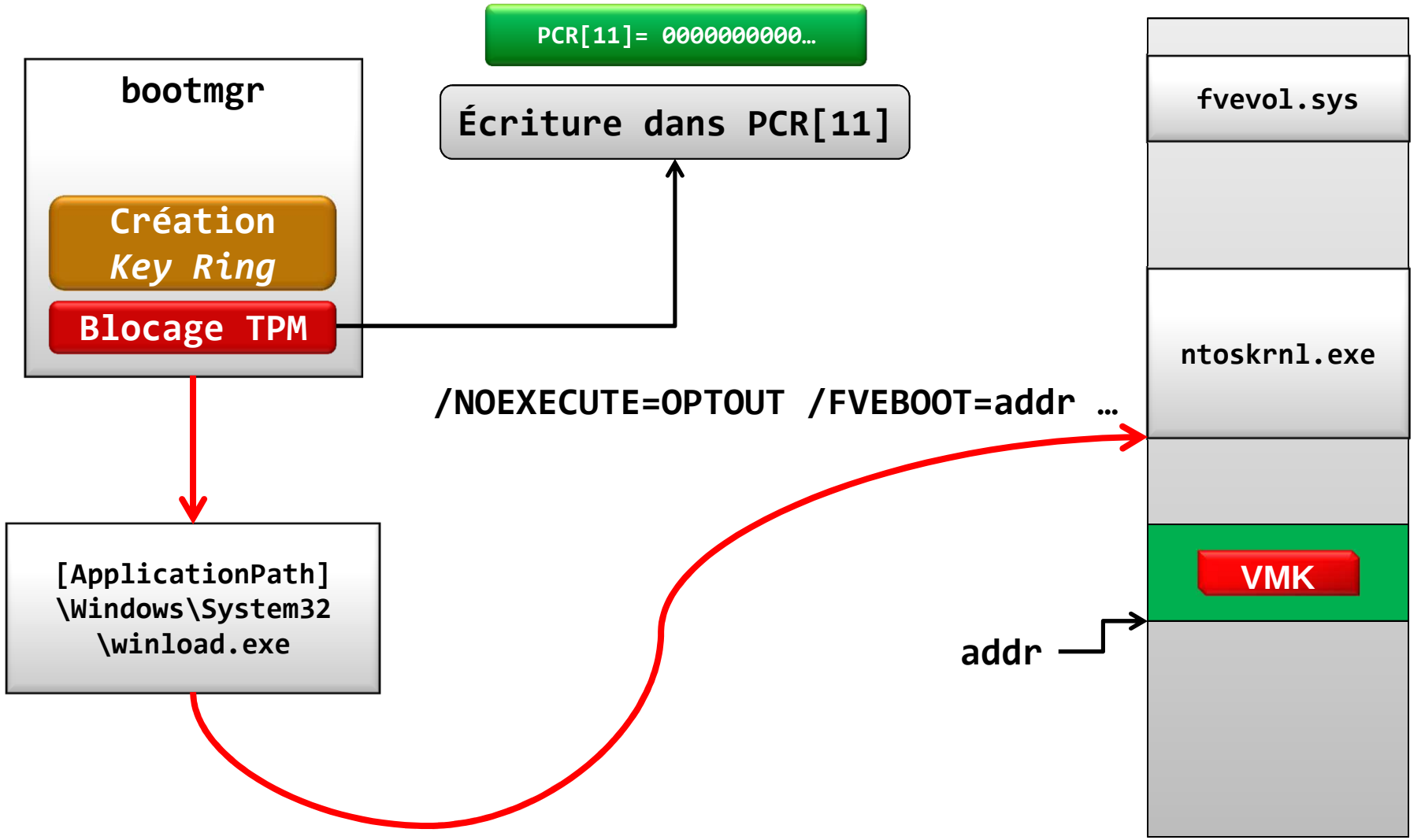
# Validation du bloc INFORMATION



# Validation de la BCD



# Fin de *bootmgr* et suite



# Membre d’un Active Directory

- L’appartenance d’une machine à un domaine permet de définir, via des GPO, des politiques :
  - de configuration (choix algorithmes, types de protecteurs VMK)
  - de sécurité (longueur des mots de passe/PIN, exigence de complexité)
  - de sauvegarde des protecteurs de récupération (clé externe, mot de passe numérique et certificat)

# Menaces sur BitLocker

# Attaques en un temps
# Ordinateur éteint

- C’est le scénario contre lequel BitLocker a été conçu

- BitLocker est efficace si :
  - Le chiffrement n’est pas suspendu
  - Les fichiers `pagefile.sys` et `hiberfil.sys` sont sur des partitions chiffrées

- Inefficacité du mode TPM seul (sans secret fourni par l’utilisateur) : possibilité de démarrer le système d’exploitation

# Attaques en un temps
# Ordinateur allumé et verrouillé

- Concerne également le mode TPM seul ou en veille *suspend to ram*
- Attaque via le réseau : exploitation de vulnérabilités, requête WMI
- Attaques physiques :
  - utilisation du « mode debug » du noyau (câble)
  - lecture de la mémoire du système : *Firewire*, PCMCIA, *Cold boot attack*, …
    - Récupération immédiate des clés via le PoolTag **FVEx**

# Attaques en un temps
# Ordinateur allumé et non verrouillé

- Concerne également l'exécution à distance de code (compromission du navigateur, fichier piégé)

- **Non Administrateurs** : aucune information pertinente récupérable (état et métadonnées *via* l'IOCTL **`IoctlFveGetDataset`**)

- **Administrateurs** :
  - Tout est possible via l'appel aux utilitaires intégrés ou via les IOCTL (**`IoctlFveGetKey`**)

# Attaques en deux temps

- Scénario de l'*evil maid* très médiatisé
- **Sans TPM, aucune protection n'est efficace**
- Avec TPM, les modifications sont détectées et l'utilisation d'un mode de récupération est proposé au démarrage (ex : modification **`bootmgr`**)
- Certaines modifications ne sont pas détectées :
  - Exemple de *phishing* : ajout d'un nouvel OS dans la BCD. Mais dans ce cas, impossibilité d'obtenir les VMK du TPM (non transmise par **`bootmgr`**)
- En cas d'anomalie au démarrage (redémarrage intempestif, entrée dans le mode de récupération), considérer le système comme compromis

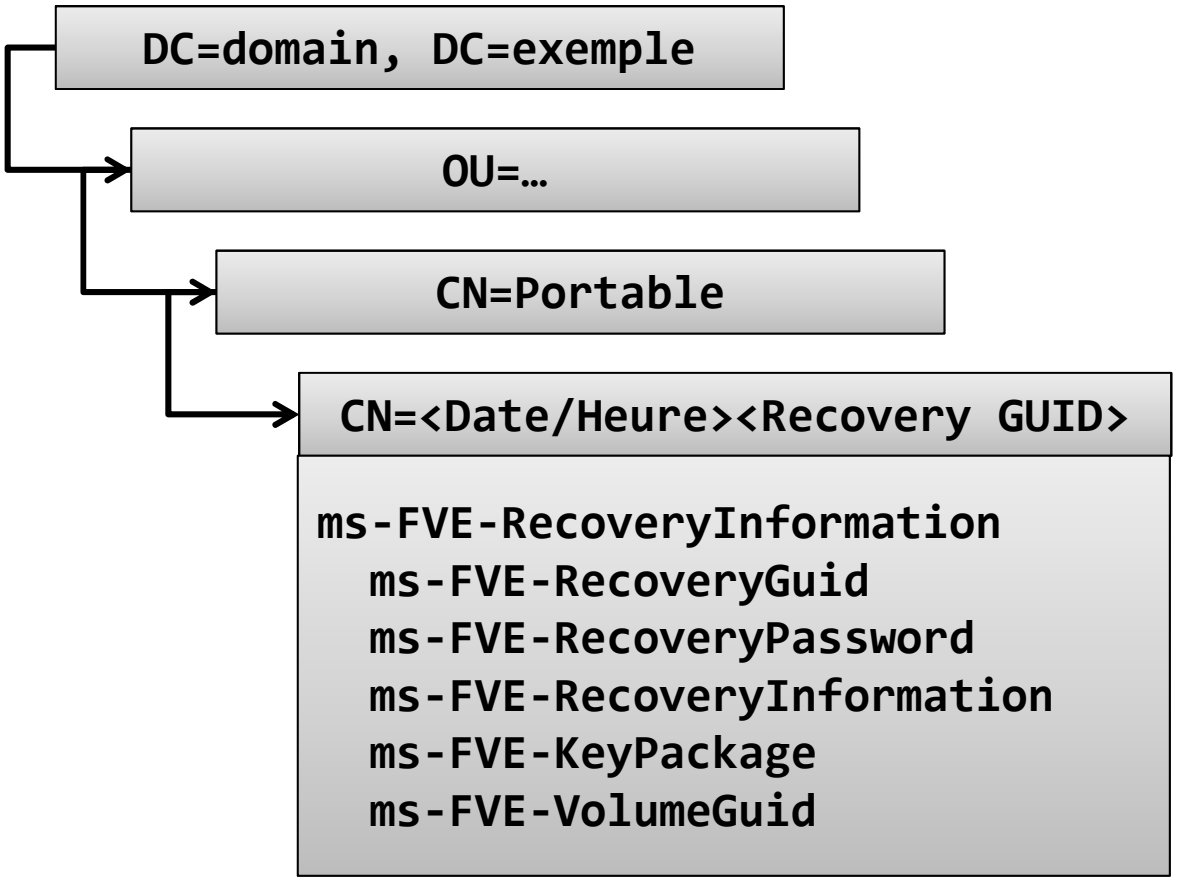
# Mode de récupération

# Analyse hors ligne

- Avec la VMK et les métadonnées, il est possible de récupérer :
  - **Clés BitLocker** : FVEK, *Auto unlock*
  - **Données des protections indirectes** :
    - Double condensat du code PIN (version non améliorée)
    - Données étirées : Mot de passe, Code Pin (version amélioré)
  - **Données de récupération** :
    - Clés externes (seule, TPM, Certificat)
    - Mot de passe numérique

# Données de récupération dans l'AD

- Sécurisée depuis Windows 2003 SP1



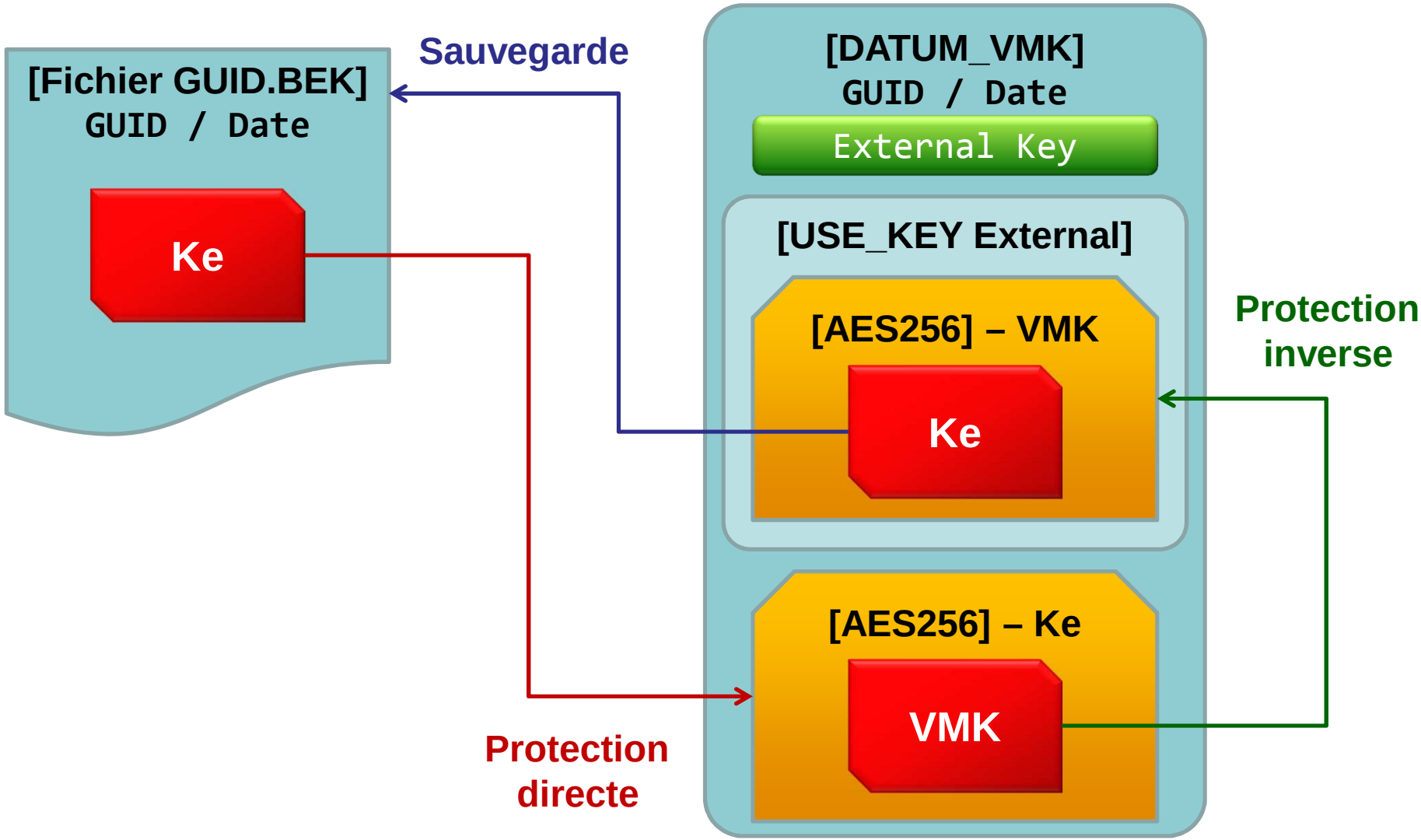

- Préférer le mode de récupération par certificat

# Conclusion

- Points positifs :
  - Stable, bien intégré au système et adapté à un contexte professionnel
  - Peut mettre en œuvre un module TPM
  - Protège efficacement contre la perte d'une machine
- Points négatifs :
  - Protection partielle de la BCD
  - Évaluation difficile de la qualité du module TPM
  - Pas dans les versions professionnelles

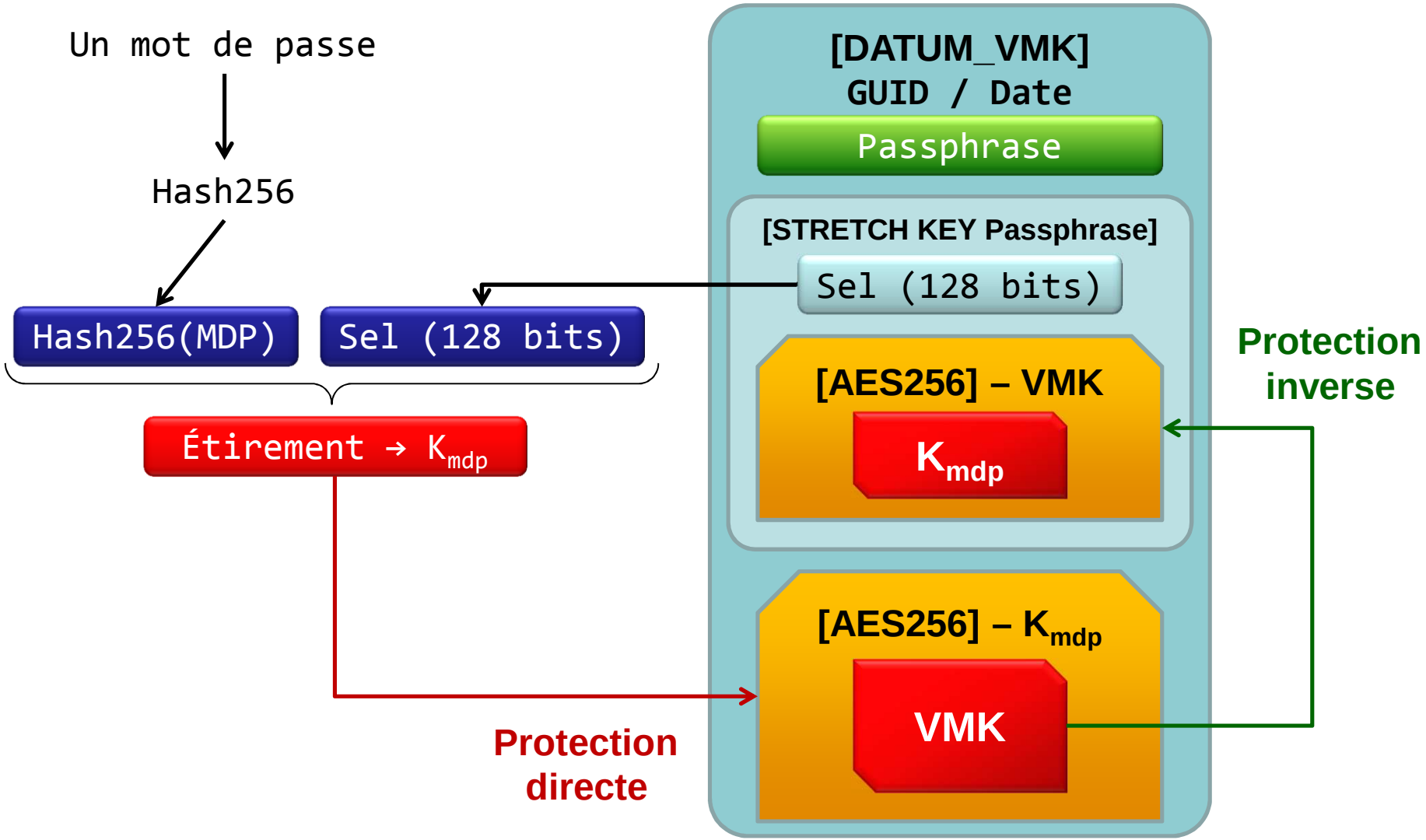
# Annexe
## Description des protecteurs VMK

# Clé externe (2)

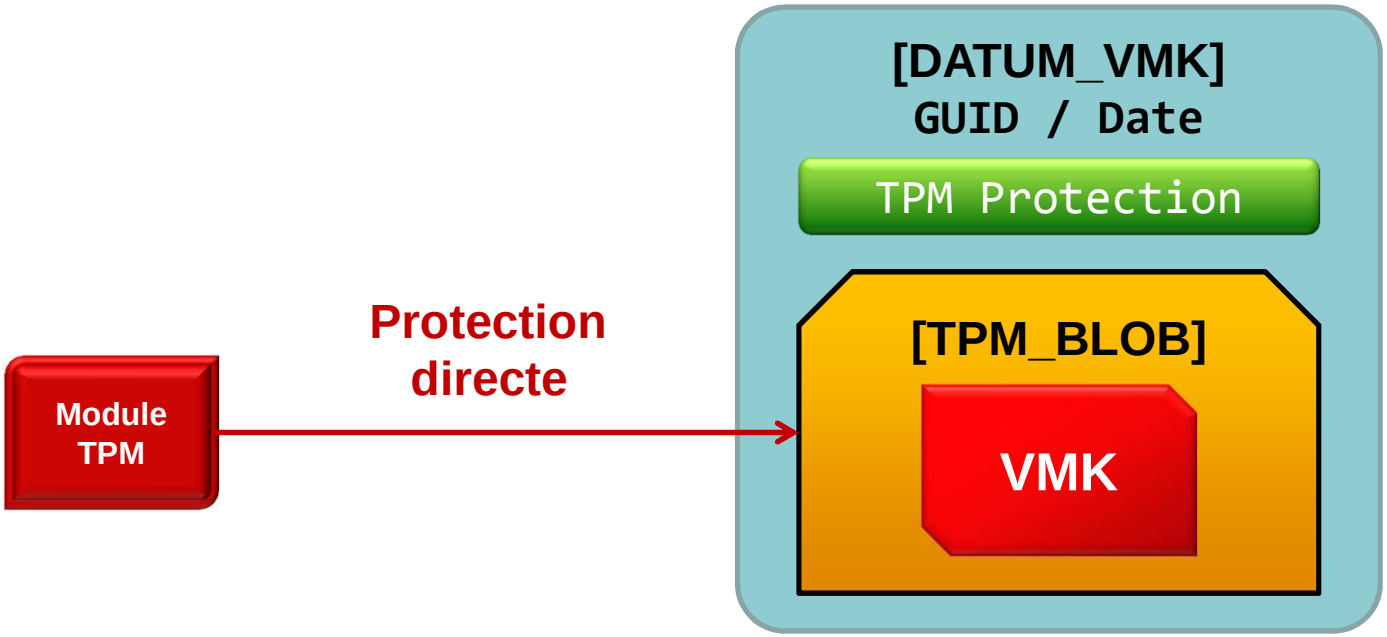


# Mot de passe (8)

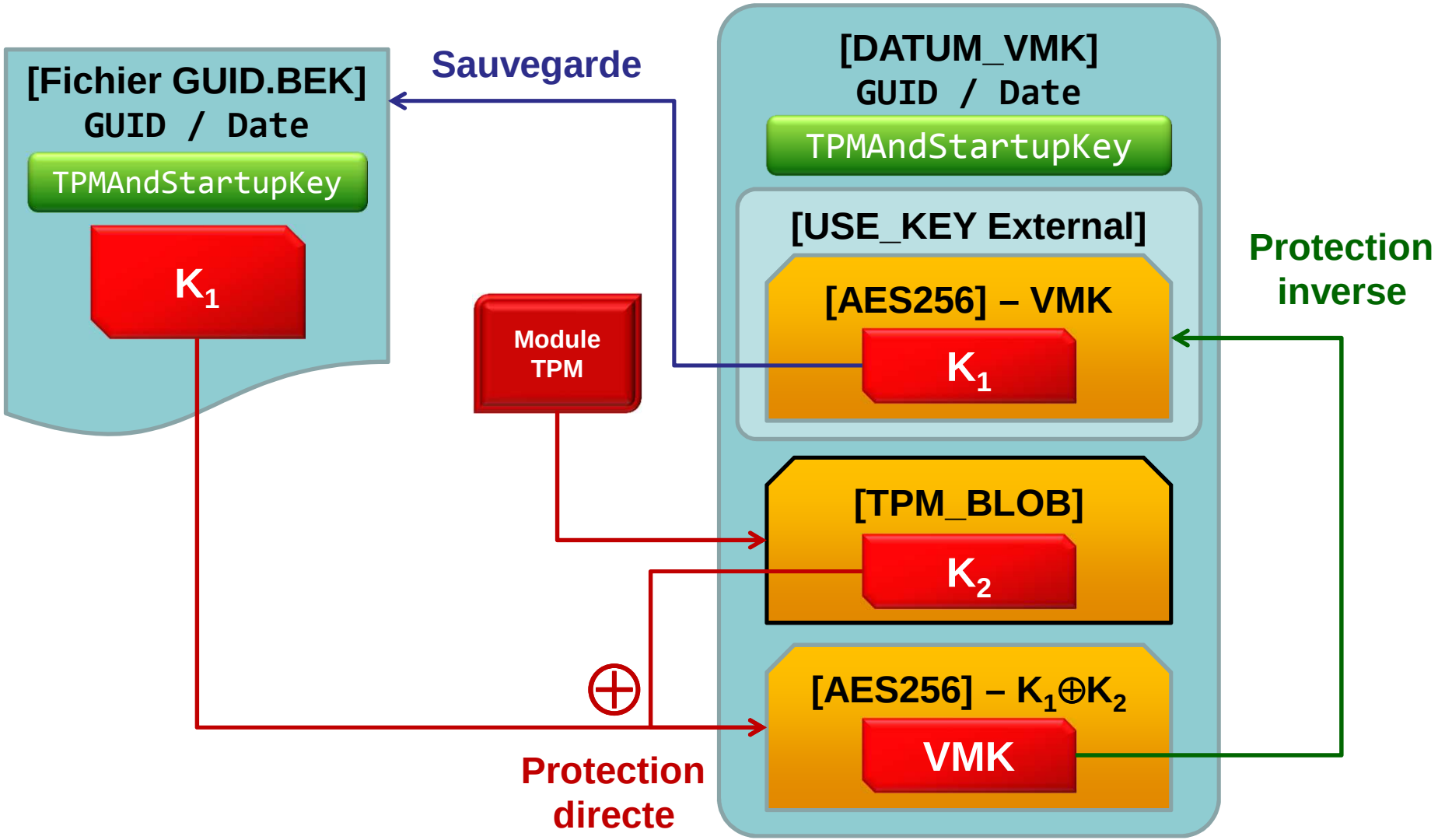
## (Passphrase, Password)



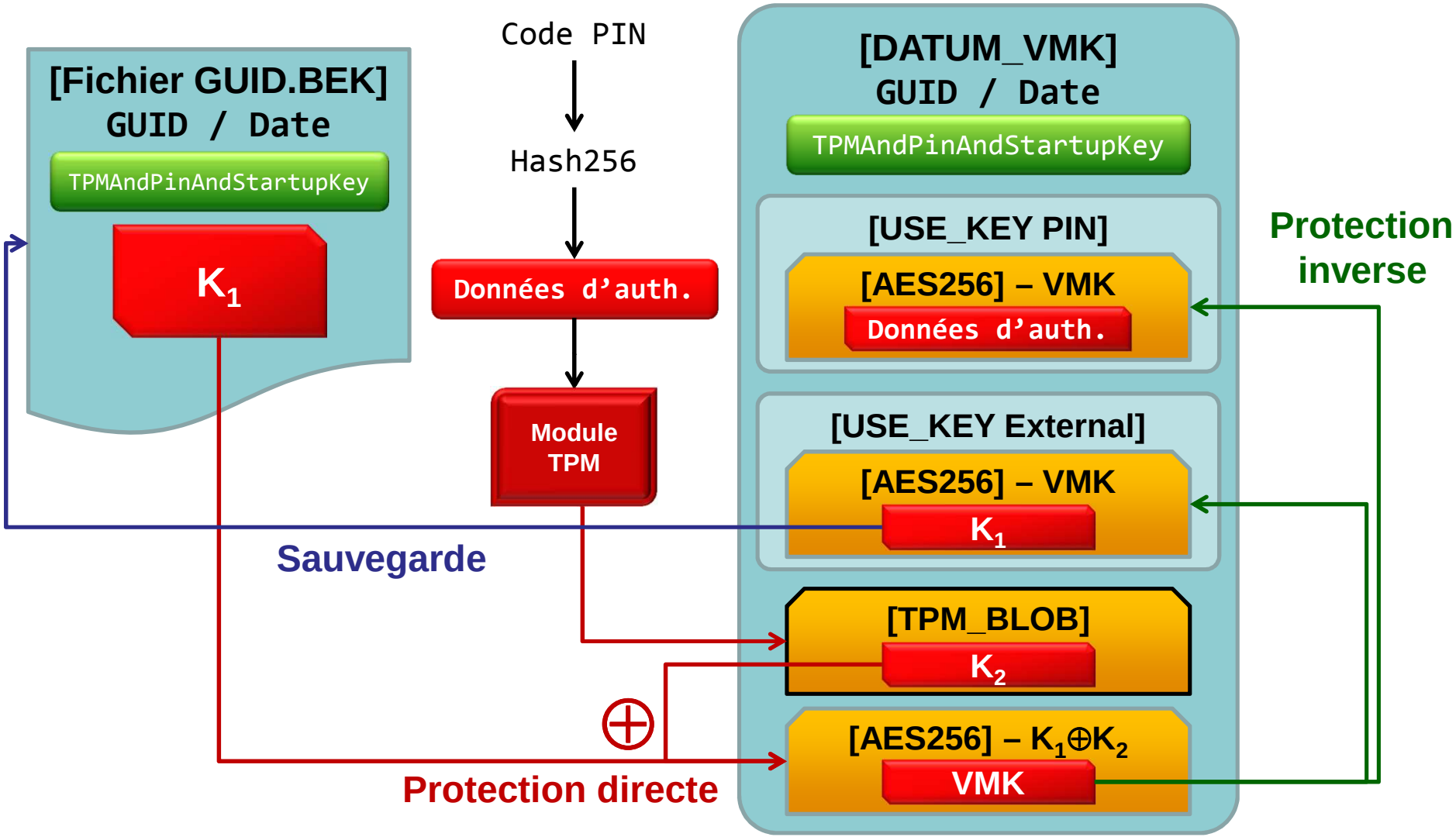
# TPM (1)


[DATUM_VMK]
GUID / Date
TPM Protection
[TPM_BLOB]
VMK
Protection directe
Module TPM

# TPMAndStartupKey (6)

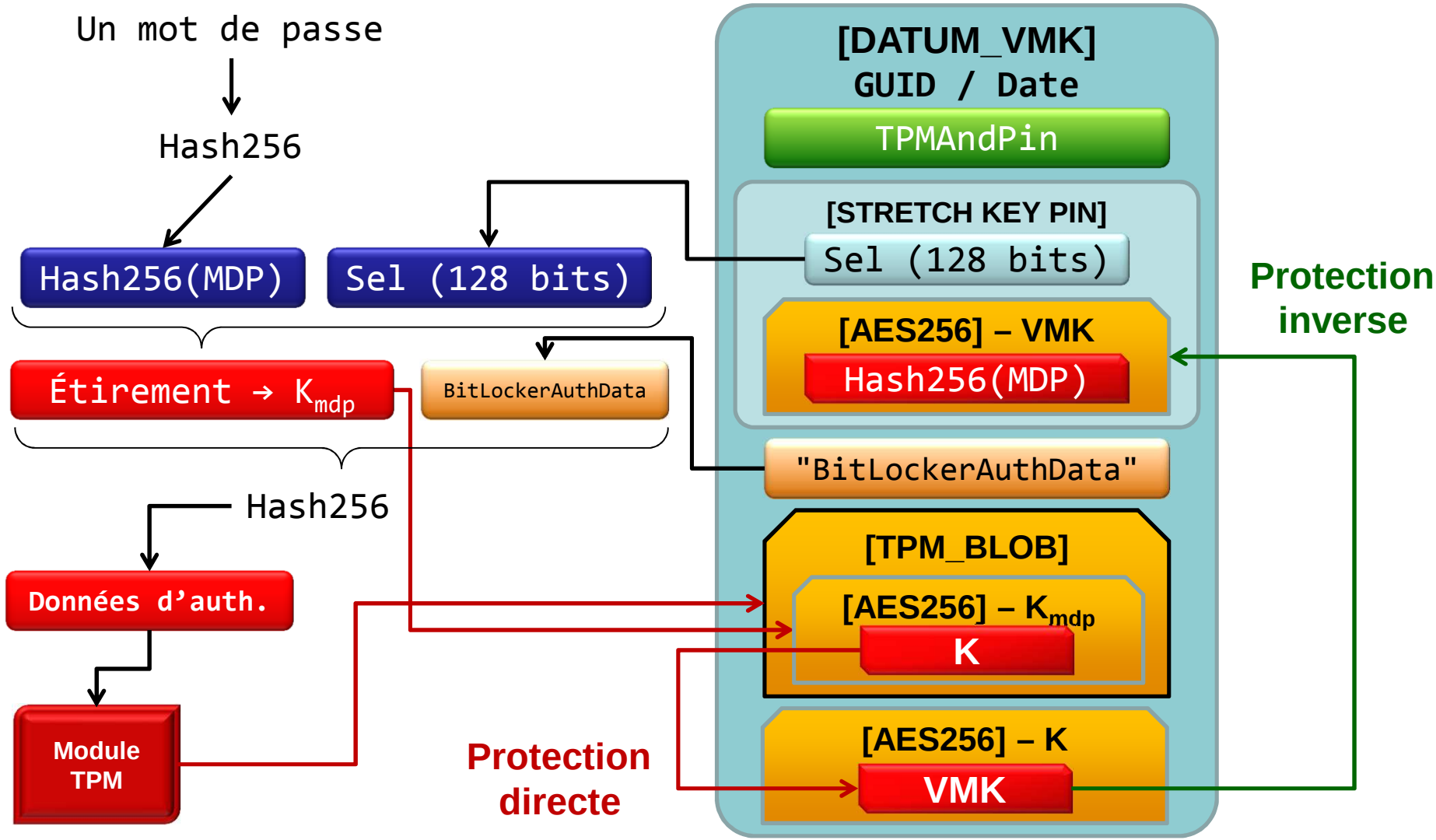


# TPMAndPINAndStartupKey (5)



# TPMAndPIN (4)

## Version code PIN amélioré



# TPMAndPINAndStartupKey (5)

## Version code PIN amélioré