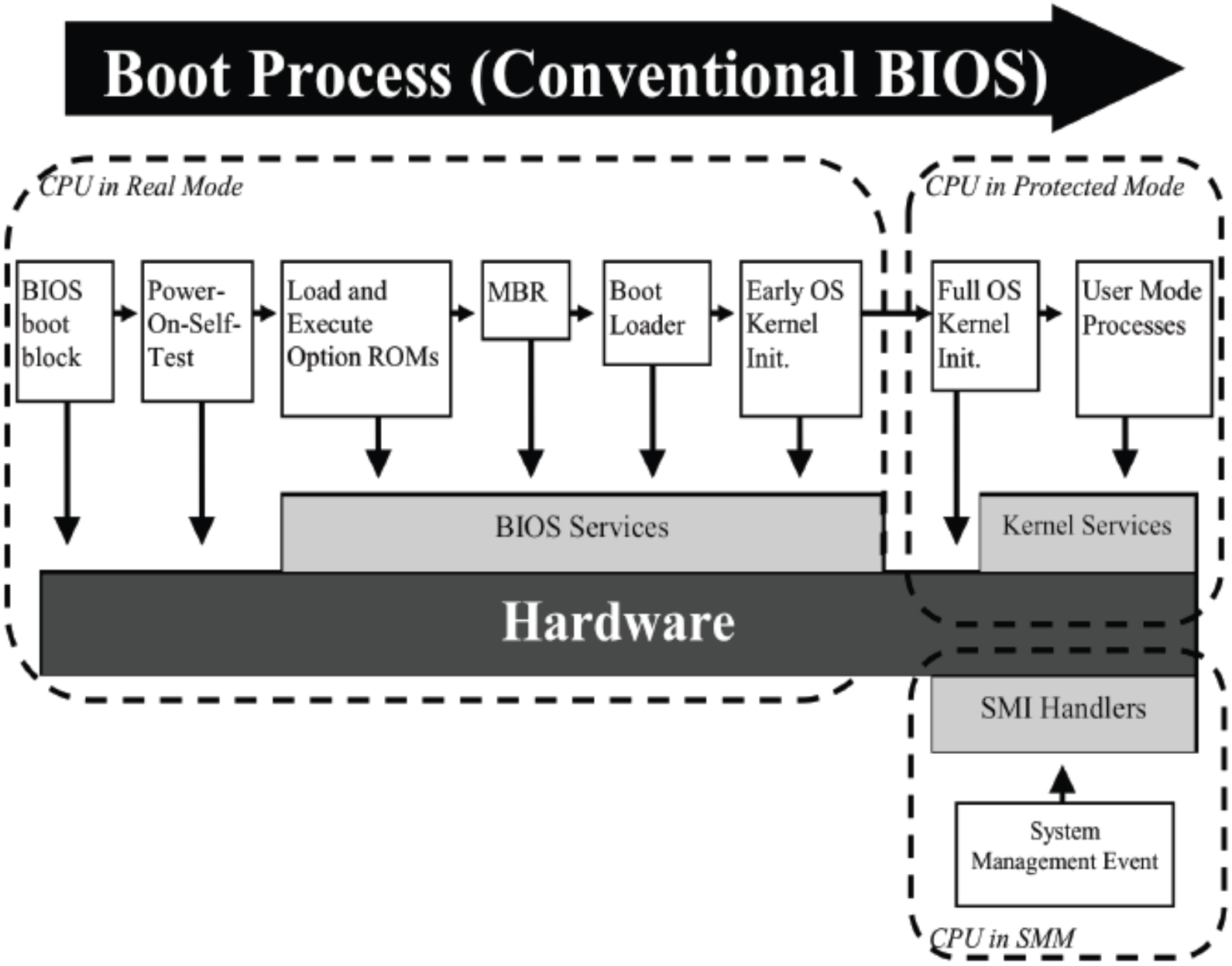
Sécurité des systèmes d'exploitation

Démarrage sécurisé

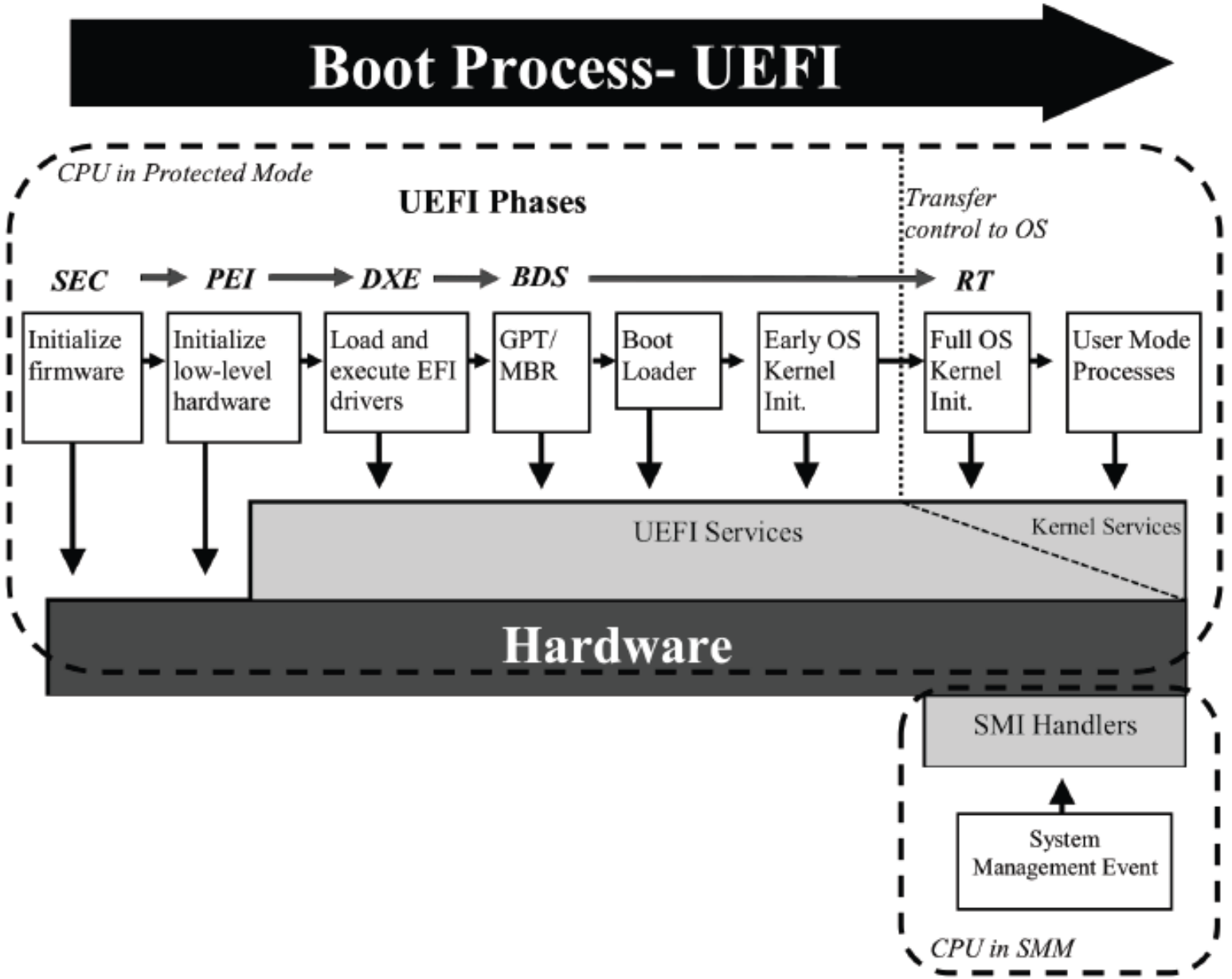
Plan

- Processus de démarrage
  - Description
  - Menaces
- Approches pour un démarrage sécurisé
  - Measured Boot TCG
  - Secure Boot UEFI
- Implémentations OS

Processus de démarrage



Processus de démarrage



Processus de démarrage

- Menaces :
  - Déni de service
  - Élévation de privilèges
    - Insertion de code dans la chaîne de démarrage afin d'insérer un rootkit dans le noyau de l'OS
    - Plusieurs points d'insertion initiaux :
      - Firmware (BIOS, UEFI, Option ROM, ...)
      - Chargeur de démarrage
      - Noyau (via le remplacement d'une partie ou l'ensemble)
      - Pilotes (pour ceux qui se chargent en espace noyau)

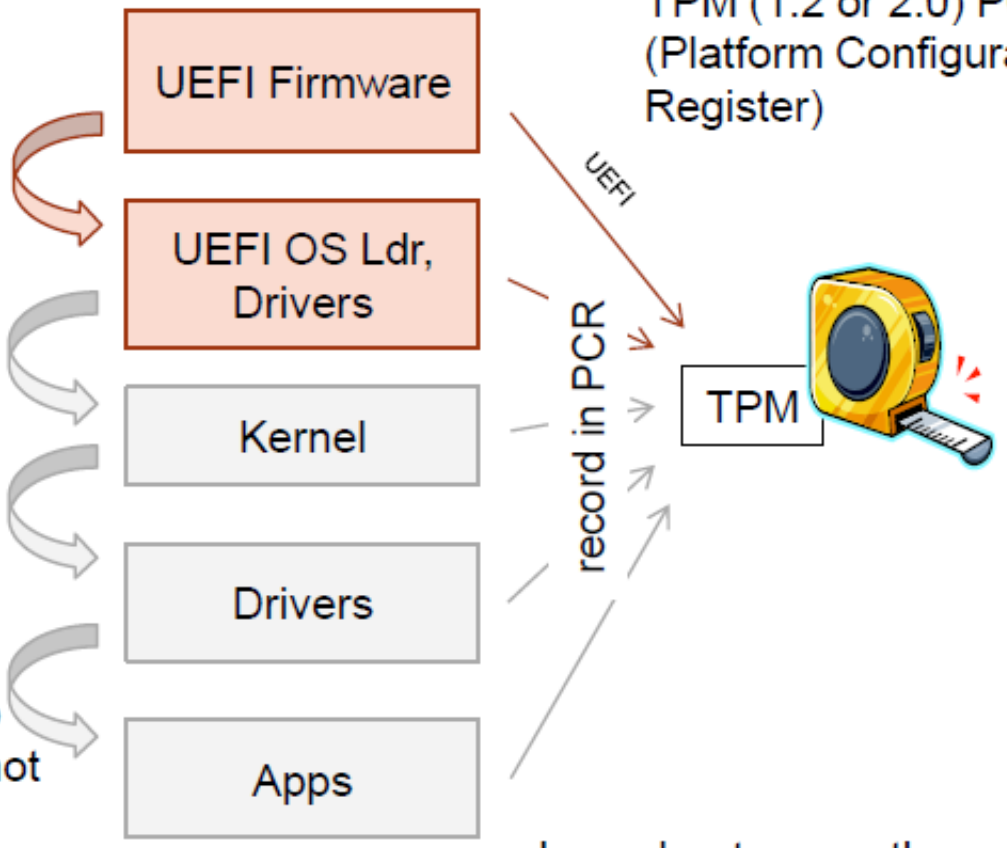
Approches pour un démarrage sécurisé

UEFI Secure Boot vs. TCG Trusted Boot

UEFI authenticate OS loader
(pub key and policy)

Check signature of before loading

- UEFI Secure boot will stop platform boot if signature not valid (OEM to provide remediation capability)
- UEFI will require remediation mechanisms if boot fails



UEFI PI will measure OS loader & UEFI drivers into TPM (1.2 or 2.0) PCR (Platform Configuration Register)

- Incumbent upon other software to make security decision using attestation

Source : Intel

Approches pour un démarrage sécurisé

- UEFI Secure Boot
  - Vérification de la signature cryptographique des binaires UEFI (format Authenticode) avant de les charger.
  - Permet de contrôler quels binaires sont autorisés
    - Par extension, limiter le chargement de malwares

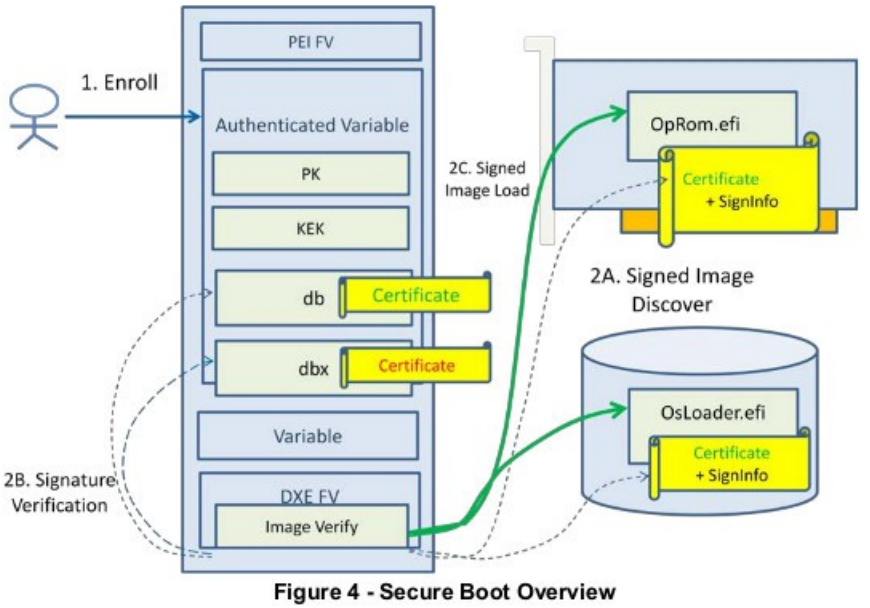
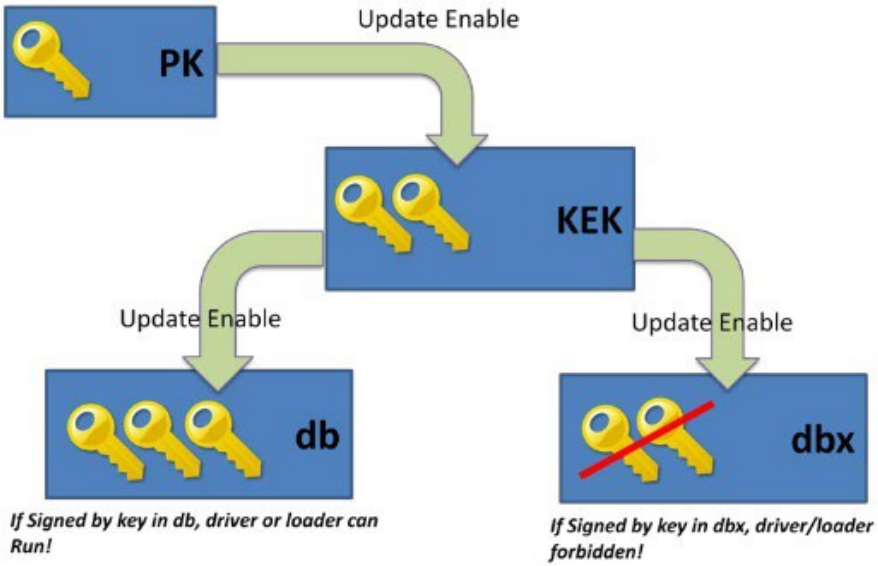


Figure 4 - Secure Boot Overview

Source : Intel

Approches pour un démarrage sécurisé

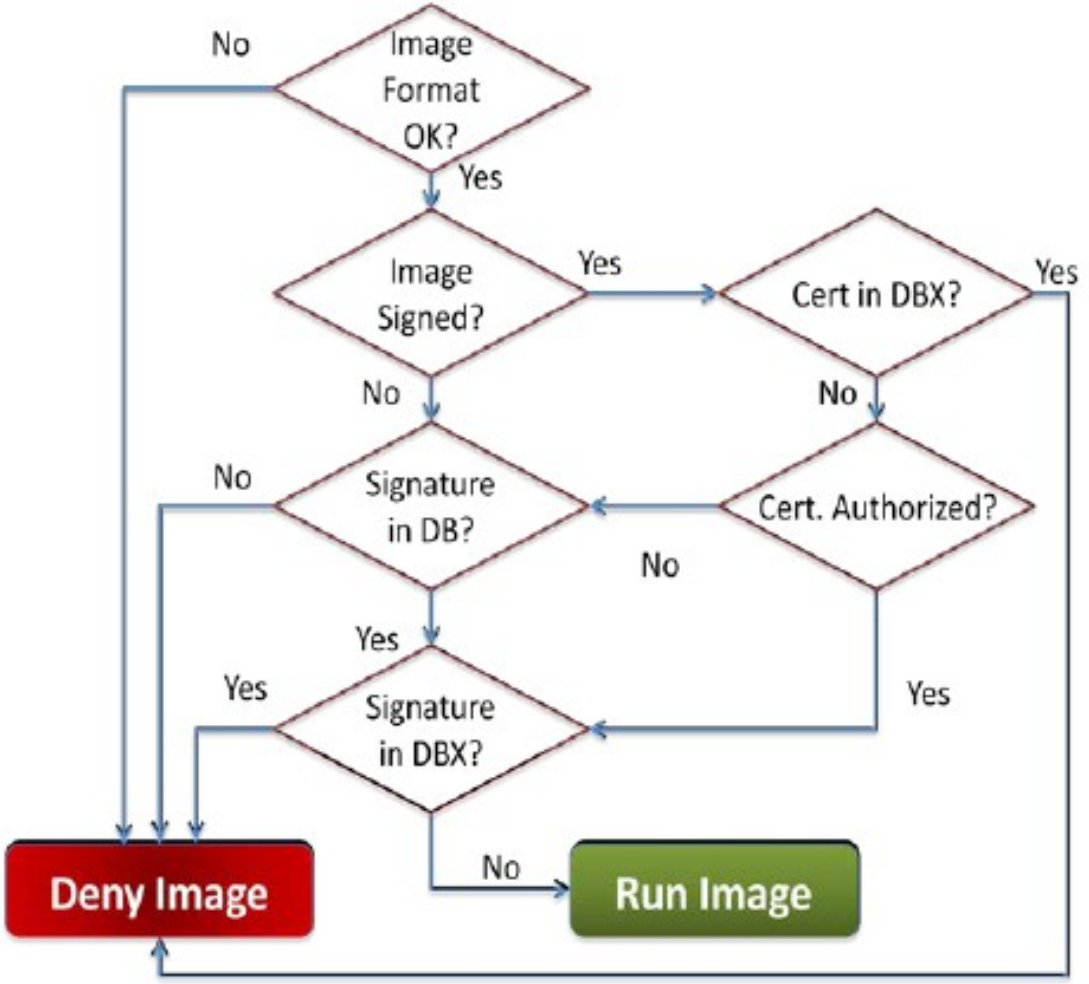
- Hiérarchie des clés
  - Platform Key (PK)
    - détenue par le propriétaire de la plateforme
    - Signature du firmware
  - Key Exchange Key (KEK)
    - propre à un système d'exploitation
    - enregistrée dans le firmware
  - 2 bases de données contenant des certificats et des hashs
    - Authorized Signatures Database (DB)
    - Forbidden Signature Database (DBX)
    - DBX est prioritaire sur DB



Source : Intel

Approches pour un démarrage sécurisé

- Vérification de la signature d'un binaire UEFI (Secure Boot activé)



Approches pour un démarrage sécurisé

- Le Secure Boot UEFI vérifie uniquement le chargeur de démarrage
- Pour établir une chaîne de confiance, il faut que chaque composant vérifie le suivant :
  - Chargeur → noyau
  - Noyau → pilotes
  - Noyau → applications
- Qui vérifie le firmware UEFI ?
  - La phase SEC (*Security*) du démarrage précède le chargement du firmware
    - Contient un bloc de code dédié qui joue le rôle de racine de confiance (*core root of trust*)

Approches pour un démarrage sécurisé

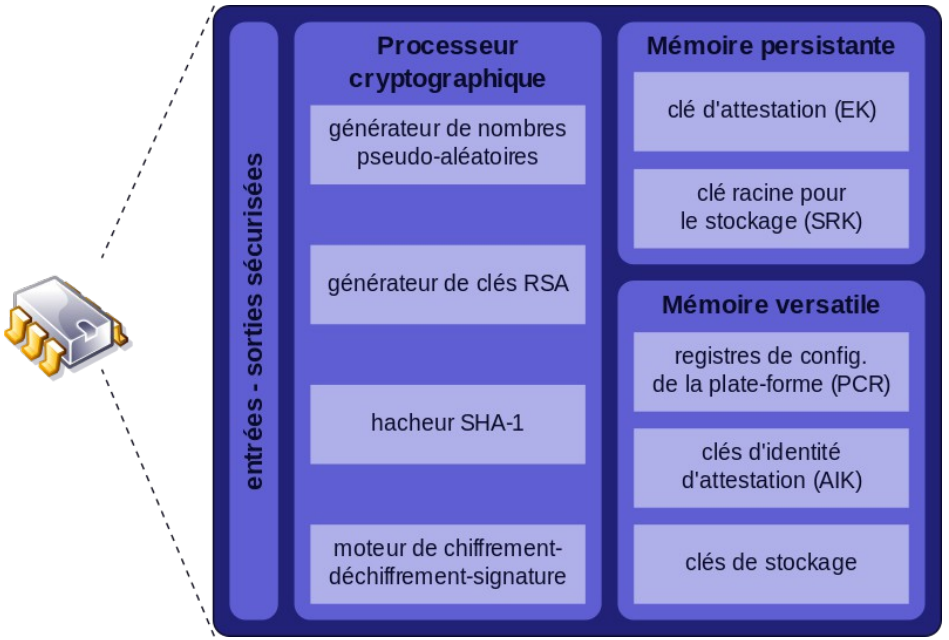
- Measured Boot du TCG (Trusted Computing Group)
  - Collection de hashs ou signatures cryptographiques associée à l'environnement de démarrage
  - Nécessite une racine de confiance de mesure : RTM (*Root of Trust for Measurement*)
  - Fournit une piste d'audit et une base pour l'attestation de l'intégrité de la plateforme
  - Protège par scellement les secrets basés sur l'intégrité de la plateforme
- Repose sur un TPM (*Trusted Platform Module*)

Approches pour un démarrage sécurisé

- TPM
  - Composant cryptographique à faible coût
  - Développement commencé fin des années 90
    - Première version déployée : TPM 1.1b (2003).
  - TPM 1.2
    - Spécifications : 2003 à 2011
    - ISO/IEC standard 11889:2009
  - TPM 2.0
    - Spécifications : 2013 à 2016
    - ISO/IEC 11889:2015
    - Parmi les évolutions : support d'algorithmes cryptographiques additionnels (*algorithm agility*)

Approches pour un démarrage sécurisé

- Fournit des capacités
  - Identification
  - Attestation
  - Gestion de clés
  - Stockage
  - Calcul de hash
  - Mesure
  - Chiffrement
- Composant passif, doit être appelé par la chaîne de démarrage

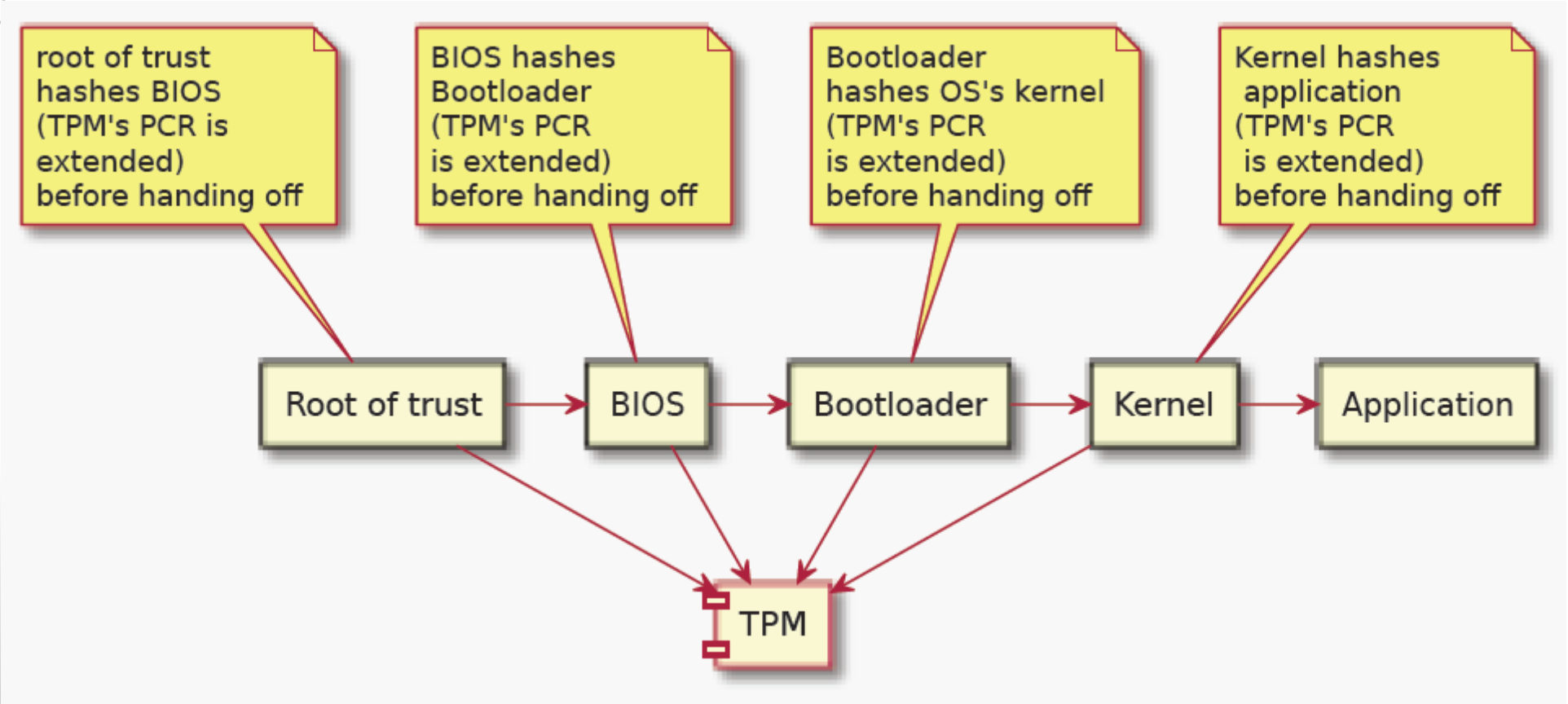


TPM 1.2 par Guillaume Piolle

Approches pour un démarrage sécurisé

- Les mesures sont stockées dans les PCR
  - Au minimum 16 PCR dans un TPM 1.2
- Pas de modification directe, 2 opérations possibles :
  - Reset
  - Extension
    - $PCR_{new} = hash(PCR_{old}||hash(data))$

Approches pour un démarrage sécurisé



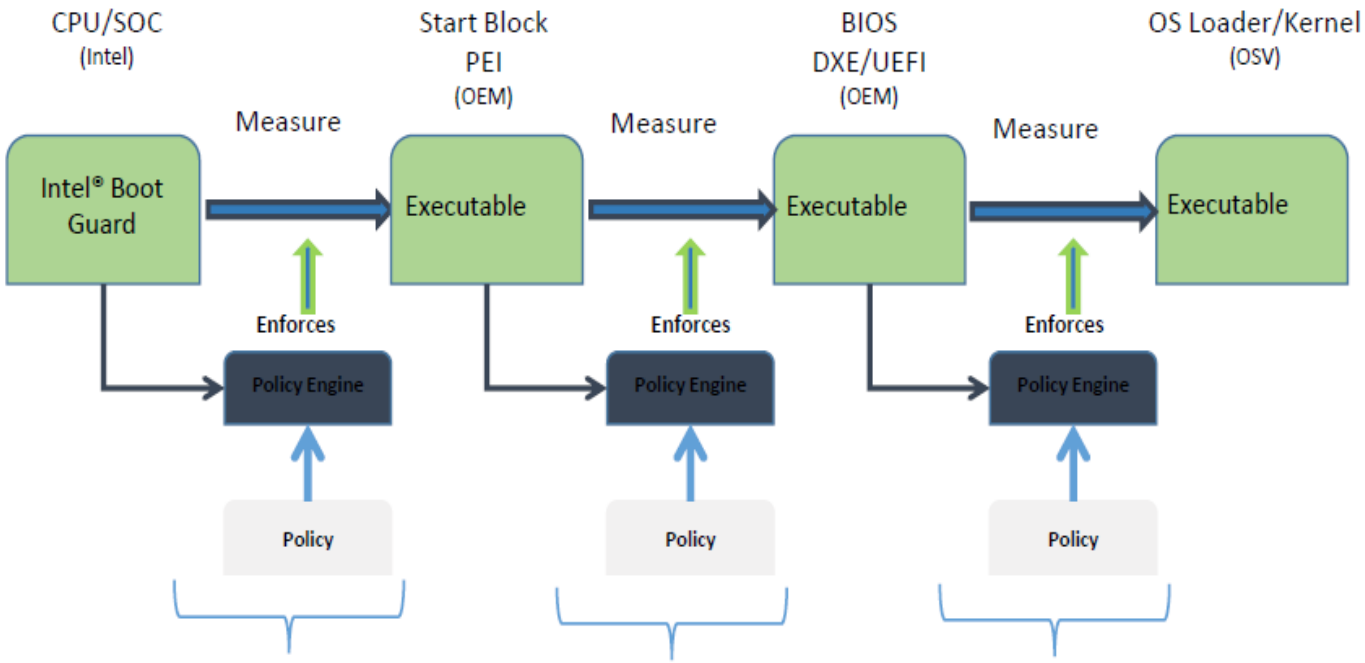
Source : 3MDEB

Approches pour un démarrage sécurisé

- Convergence
  - Trusted Execution Environment TrEE (1.0)
  - Protocole EFI qui permet de :
    - Vérifier la capacité du firmware à interagir avec le TPM
    - Obtenir le journal du Measured Boot TCG
    - Ajouter des mesures au journal et étendre les PCR du TPM
    - Transmettre des commandes au TPM

Approches pour un démarrage sécurisé

- Convergence vue par Intel
  - Secure Boot + Measured Boot



Intel® Device Protection Technology with Boot Guard

http://www.intel.com/content/dam/www/public/us/en/documents/product-briefs/4th-gen-core-family-mobile-brief.pdf

OEM PI Verification Using PI Signed Firmware Volumes

Vol 3, section 3.2.1.1 of PI 1.3 Specification

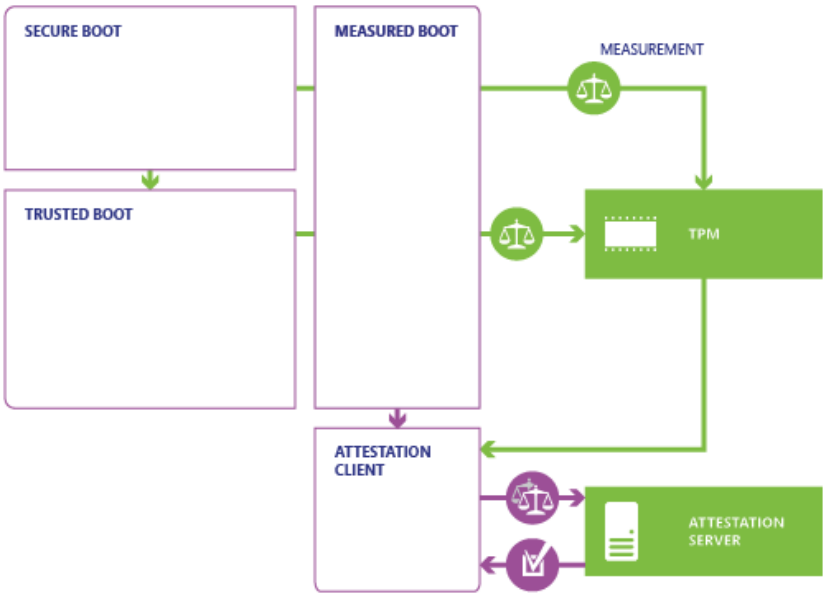
OEM UEFI 2.7 Secure Boot

Chapter 27.2 of The UEFI 2.4 Specification

Source : Intel

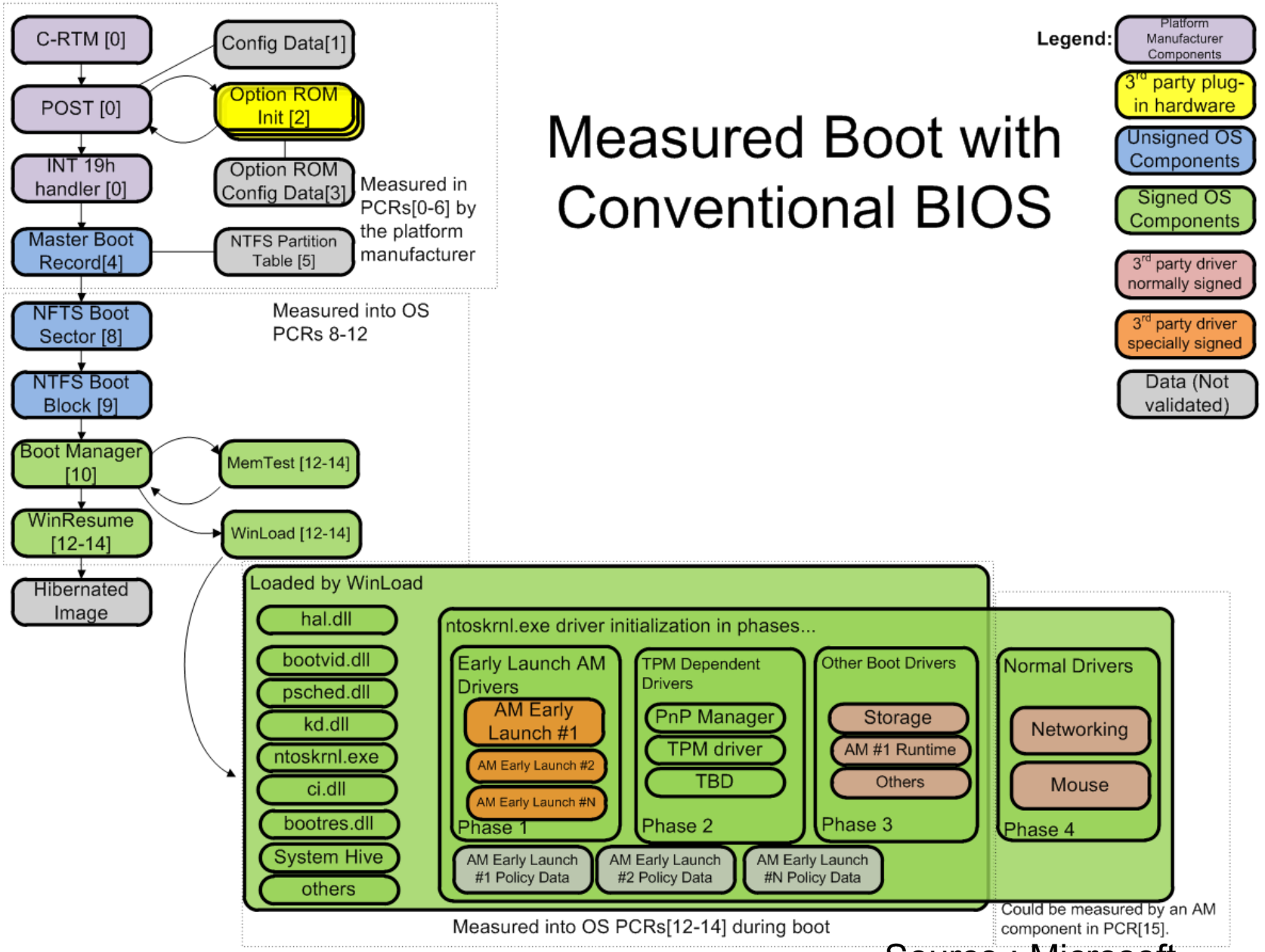
Implémentations OS

- Windows (>= 8)
  - Prise en compte du Secure Boot UEFI et du Measured Boot du TCG
  - Trusted Boot : étapes de vérification qui suivent le Secure Boot UEFI
  - Les mesures peuvent être envoyées vers un serveur d'attestation



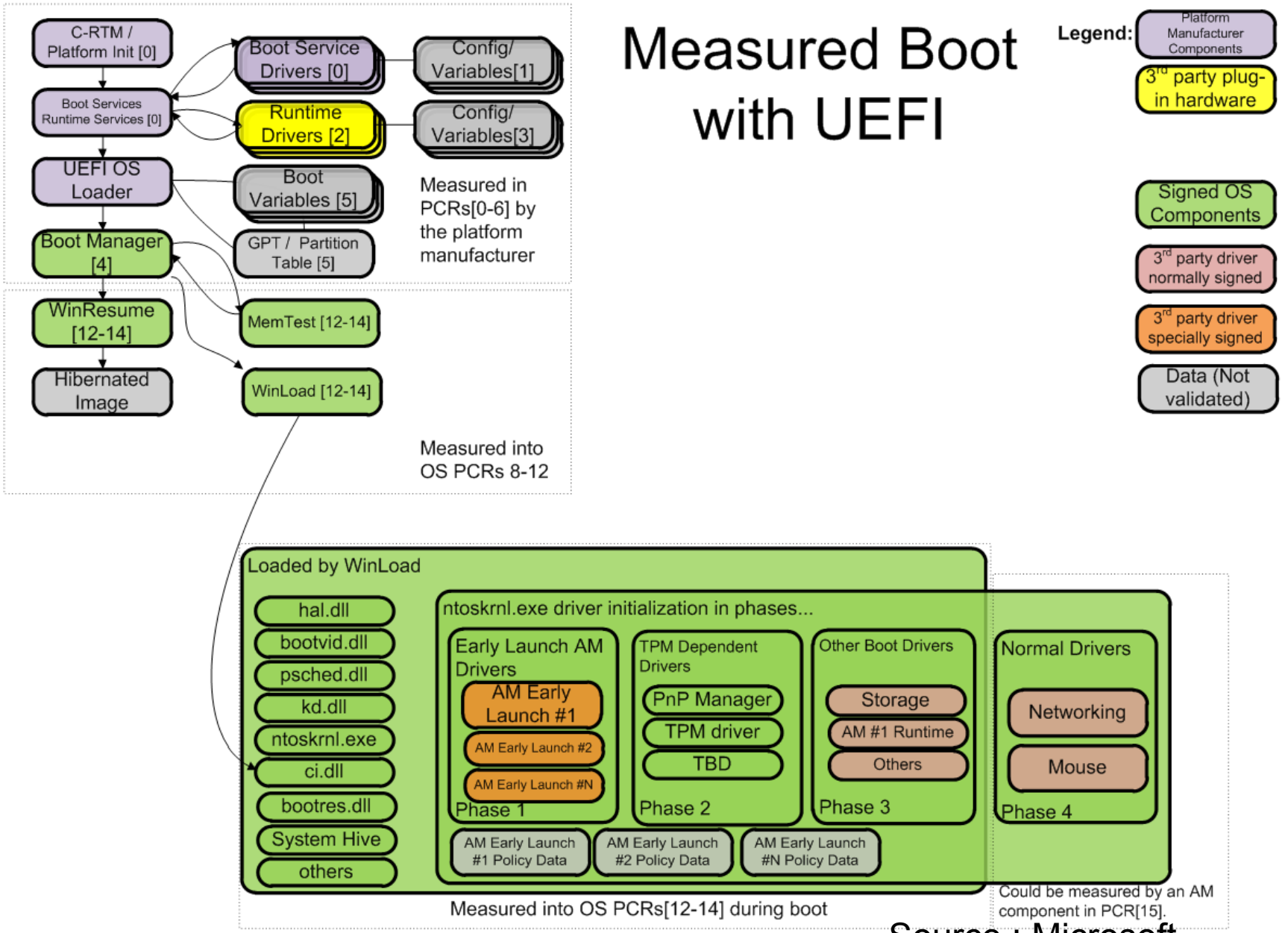
Source : Microsoft

Implémentations OS



Source : Microsoft

Implémentations OS



Source : Microsoft

Implémentations OS

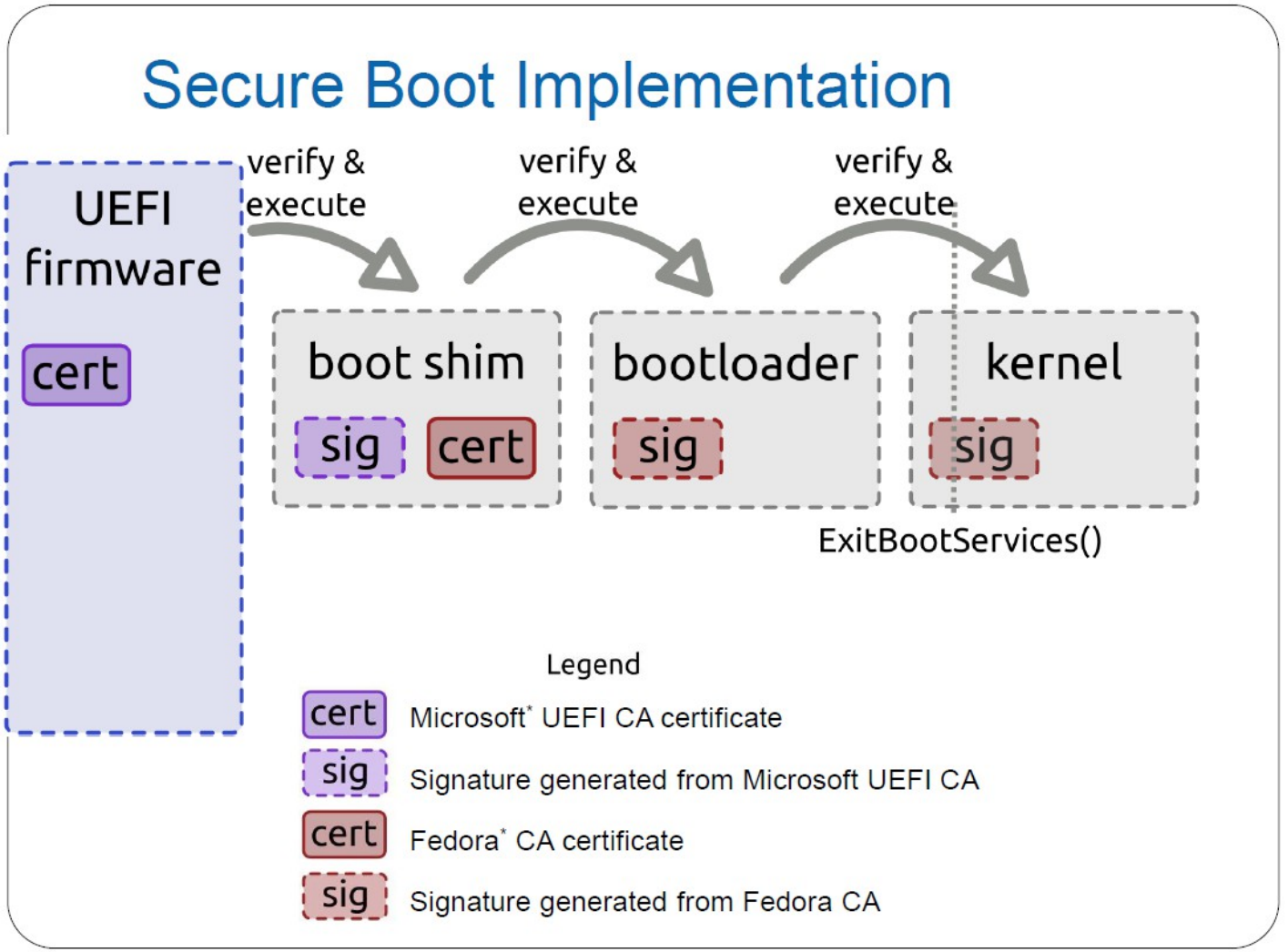
- Support du Measured Boot TCG par les systèmes Linux
- Inventaire non-exhaustif
  - Tboot (Intel)
    - https://sourceforge.net/projects/tboot/
    - Support UEFI via GRUB2
  - Trusted Grub 2 (Rohde & Schwarz)
    - https://github.com/Rohde-Schwarz-Cybersecurity/TrustedGRUB2
    - Pas de support UEFI

Implémentations OS

- Support du Secure Boot UEFI par les systèmes Linux
- Plusieurs approches
  - Créer les clés PK, KEK et les bases DB et DBX, puis signer la chaîne de démarrage
    - https://www.wzdftpd.net/blog/uefi-secureboot-debian.html
  - Utiliser un binaire (shim.efi) signé par Microsoft
    - Constat : KEK Microsoft présente par défaut dans la plupart des machines vendues
    - shim.efi vérifie Grub2, Grub2 vérifie le noyau
    - grubx64.efi et le noyau sont signés par une clé de distribution insérée dans shim.efi

Implémentations OS

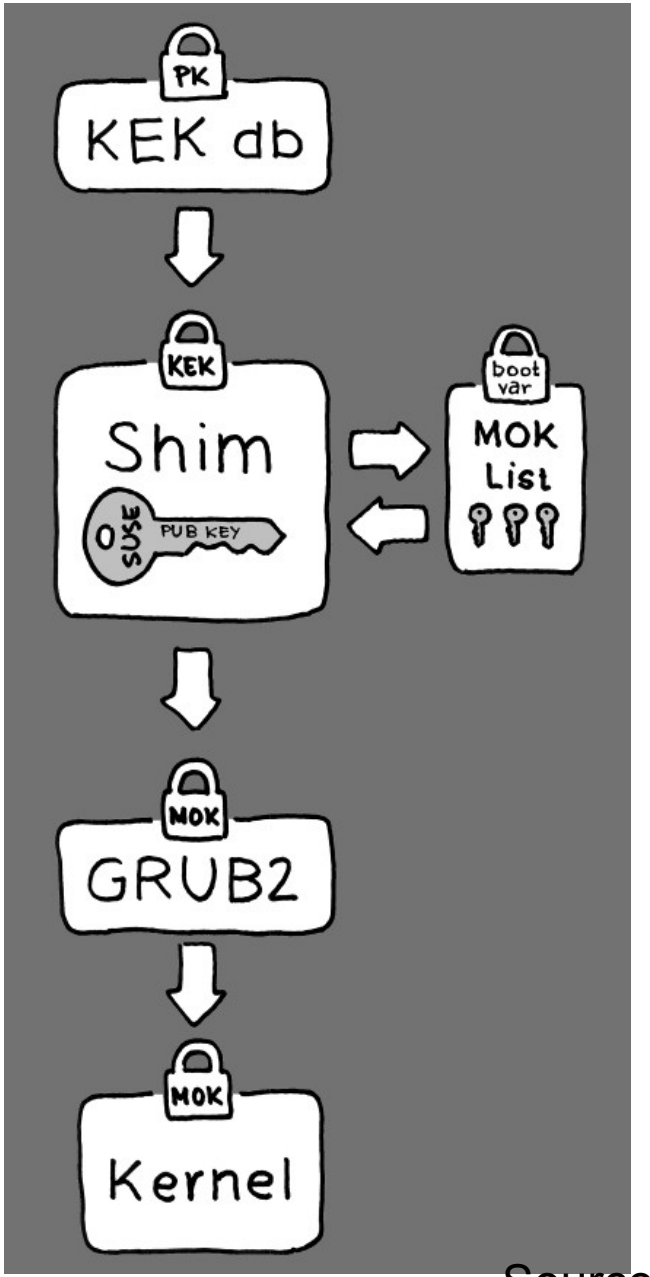
- Illustration de l'approche SHIM



Source : Intel

Implémentations OS

- Dernière approche
  - Utiliser une autre version (shim.efi) signé par Suse
    - Fonctionne sur les machines où la KEK Suse a été signée par les constructeurs
    - Ajoute une autre base de clés (*Machine Owner Key*)
    - Grub2 et le noyau sont signés avec une clé MOK



Source : Suse

Implémentations OS

- Travaux de convergence
  - Intégration de mesure TPM dans le chargeur SHIM
    - https://github.com/rhboot/shim
  - Measured and verified boot in UEFI Grub2 with TPM2 (Matthew Garrett)
    - http://lists.gnu.org/archive/html/grub-devel/2017-07/msg00003.html

Pour aller plus loin

- Advanced x86: Introduction to BIOS & SMM
  - http://opensecuritytraining.info/IntroBIOS.html
- Introduction To Trusted Computing
  - http://opensecuritytraining.info/IntroToTrustedComputing.html
- Secured Boot and Measured Boot: Hardening Early Boot Components against Malware, Microsoft, 2012
- Firmware is the new Black –Analyzing Past 3 years of BIOS/UEFI Security Vulnerabilities, Monroe & al., Black Hat USA 2017

Questions ?