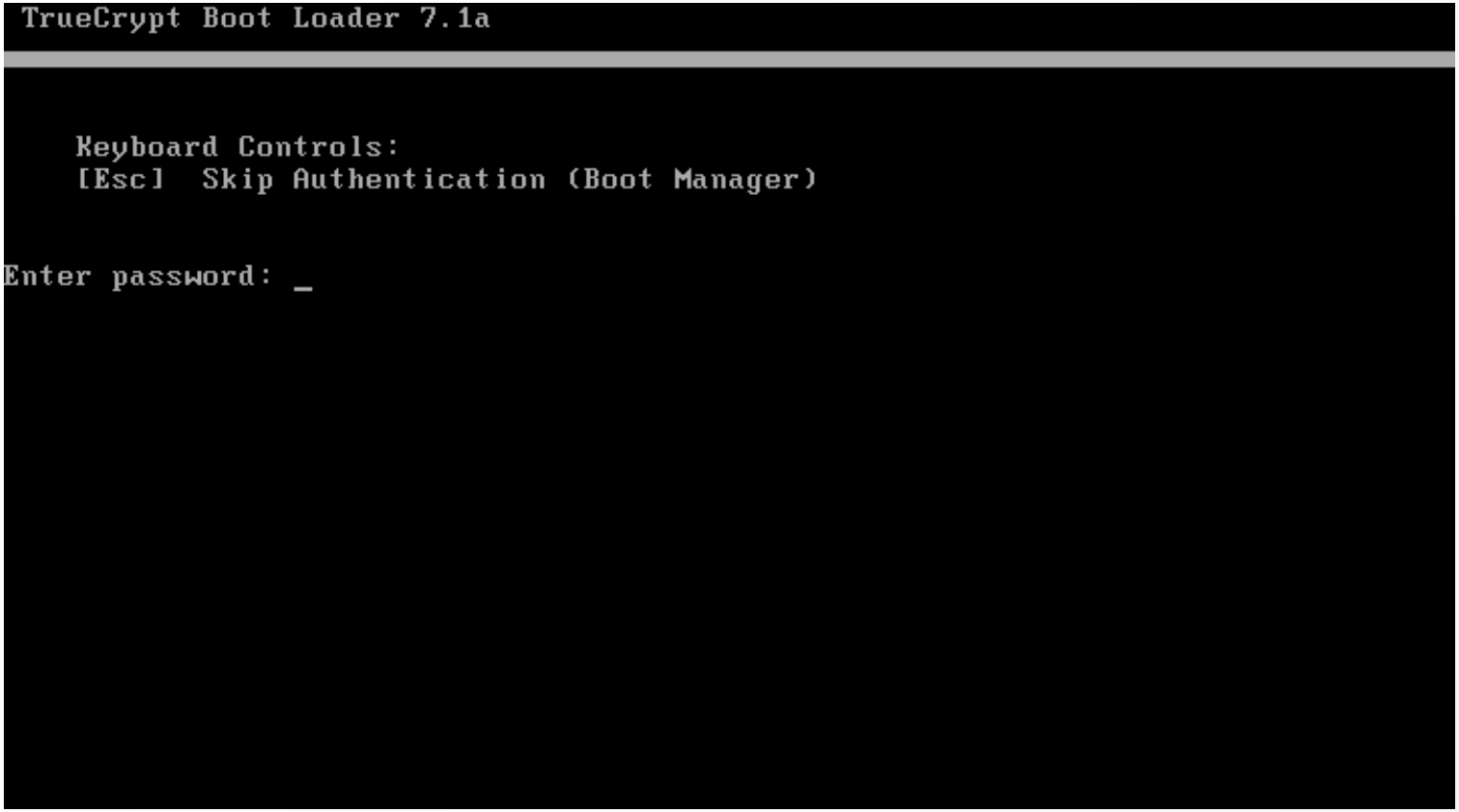
Attestation distante d'intégrité sous Android

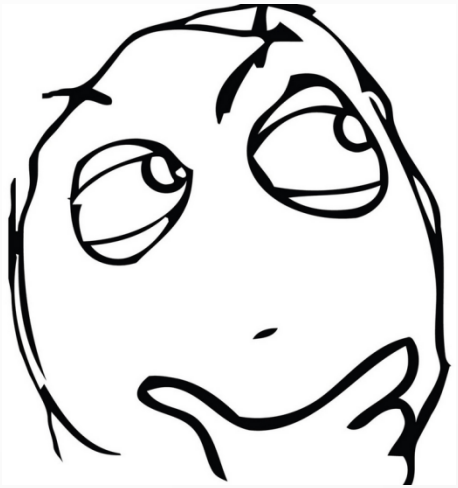
Dimitri Kirchner – @Tibapbedoum
AMOSSYS

Ingénieur sécurité à AMOSSYS

Android
Informatique de confiance

Source :
http://favim.com/image/49365/

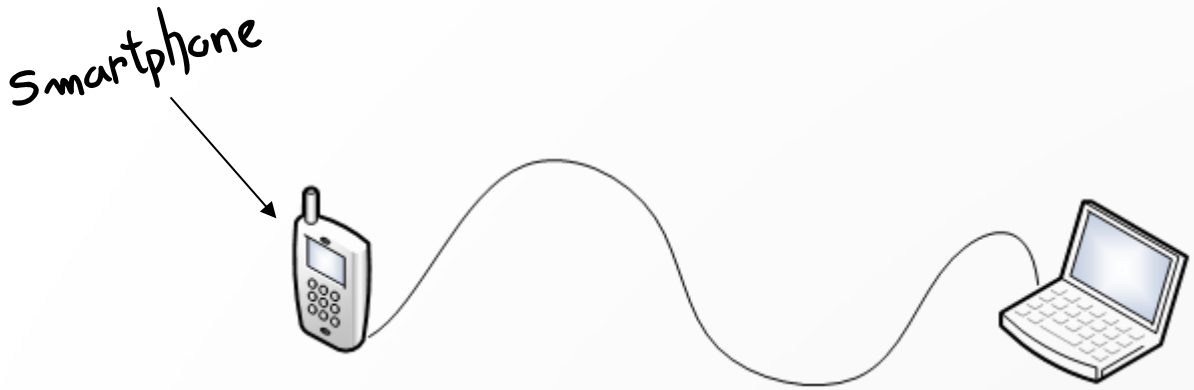

TrueCrypt Boot Loader 7.1a
Keyboard Controls:
[Esc] Skip Authentication (Boot Manager)
Enter password: _



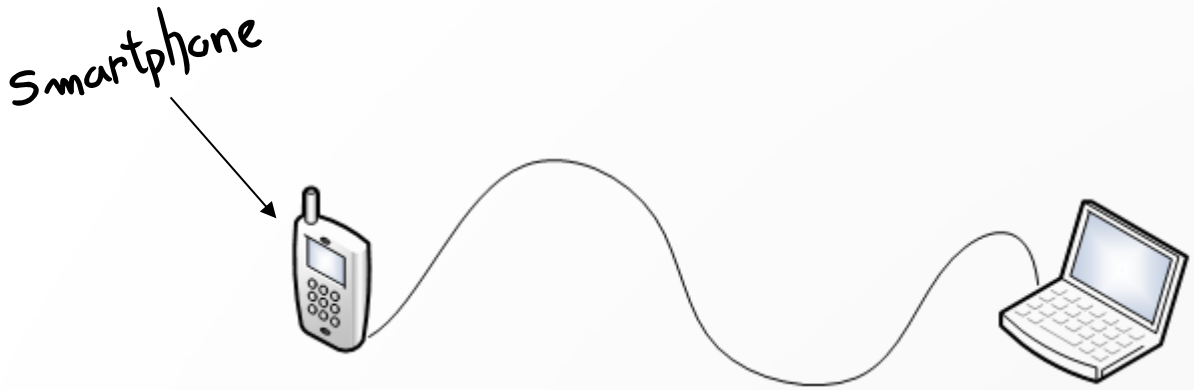
Un ordinateur avec un TPM…

Un téléphone…

Hypothèse :
Le téléphone est de confiance



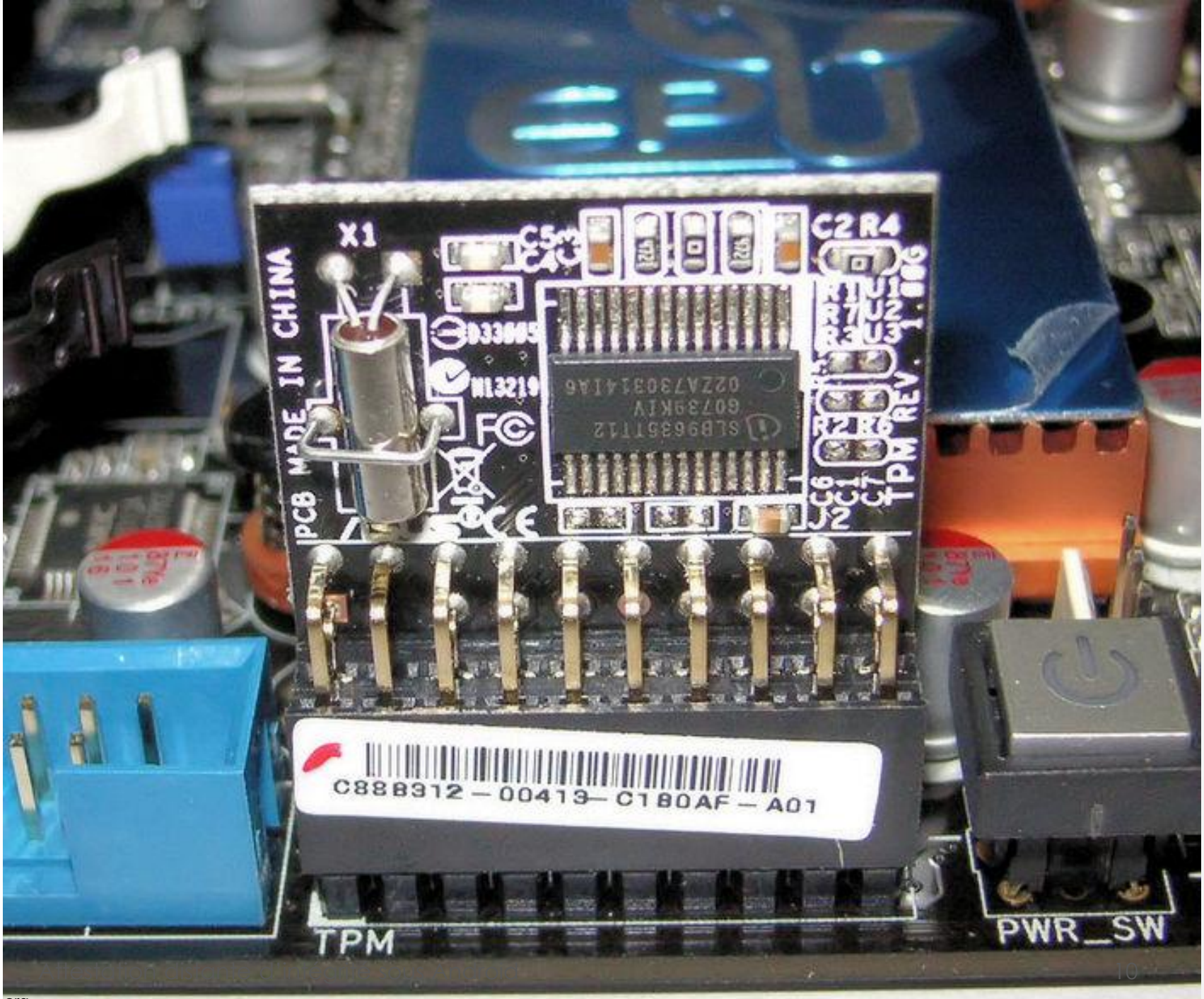
- Étape 1 : L'utilisateur connecte son *smartphone*
- Étape 2 : Le poste utilisateur prouve son intégrité au *smartphone*
- Étape 3 : L'utilisateur prend une décision



- Étape 1 : L'utilisateur connecte son *smartphone*
- **Étape 2 : Le poste utilisateur prouve son intégrité au *smartphone***
- Étape 3 : L'utilisateur prend une décision

Quelques rappels sur l'informatique de confiance

- Attester de l'intégrité d'un logiciel
- *Trusted Computing Group*
- *Trusted Platform Module*



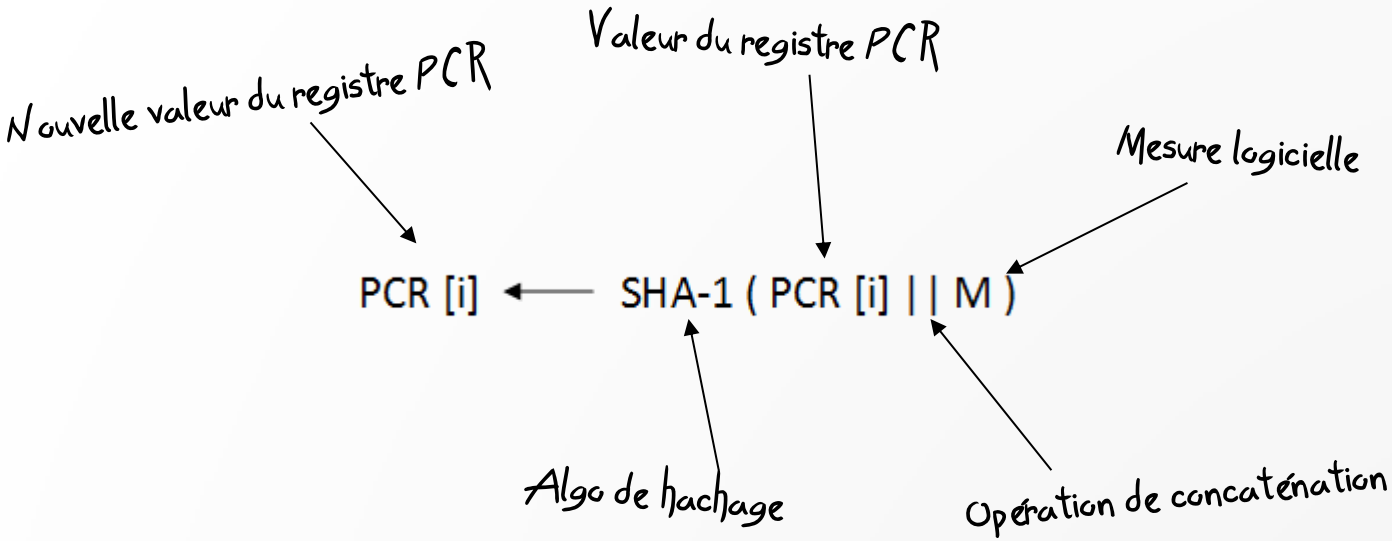
Source : Wikipedia.org

Trusted Platform Module

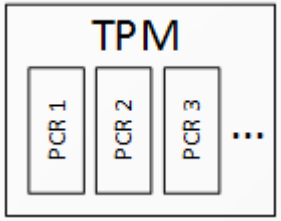
- Fonctions cryptographiques
- Stockage sécurisé
- Mécanisme d'agrégation de mesures

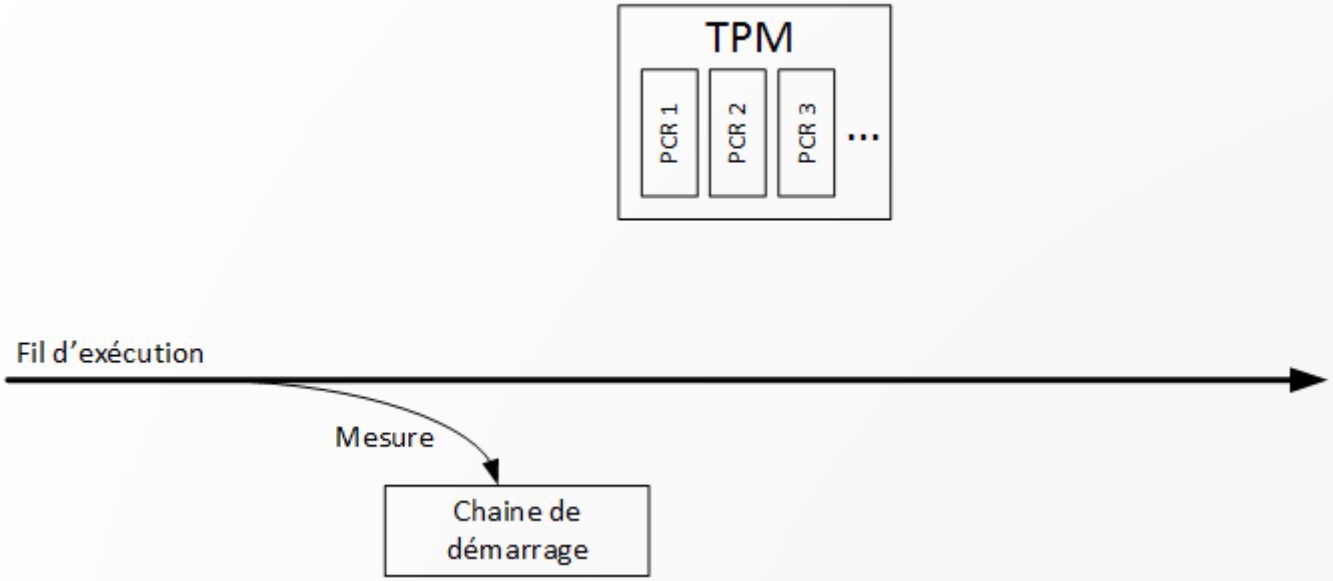
Registres PCR

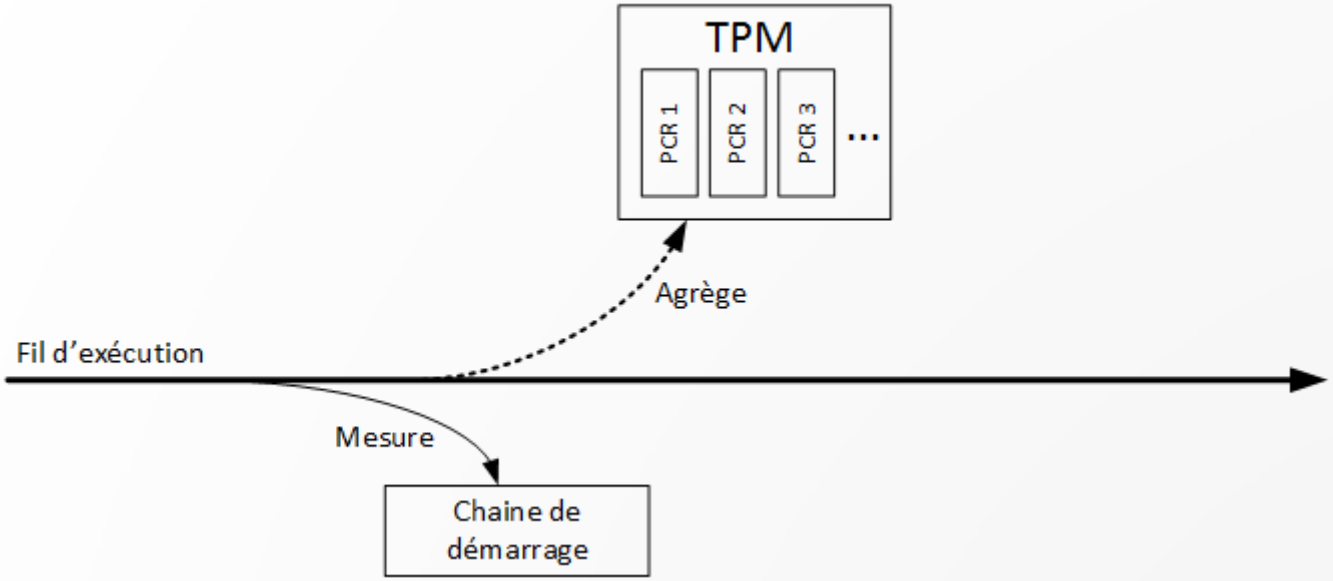
- *Platform Configuration Registers*
- Mémoires internes au TPM
- Contiennent les mesures agrégées

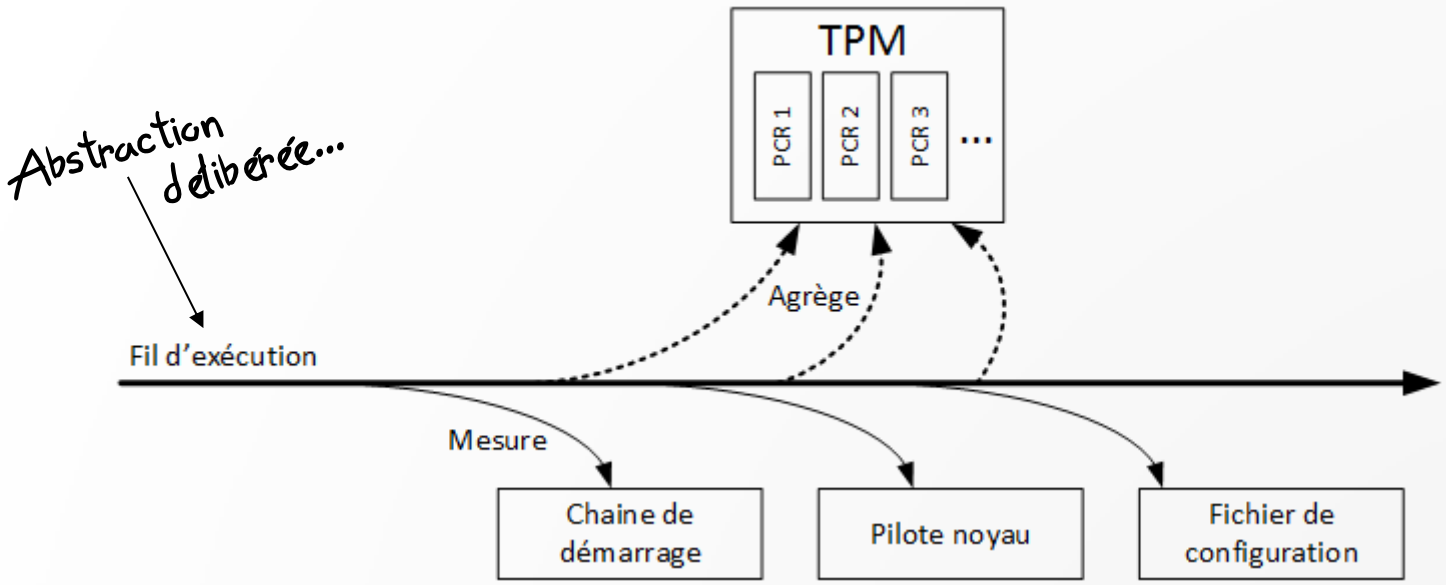


Permet de caractériser l'intégrité d'une plateforme


TPM
PCR 1
PCR 2
PCR 3
...


TPM
PCR 1
PCR 2
PCR 3
...
Fil d'exécution
Mesure
Chaine de démarrage

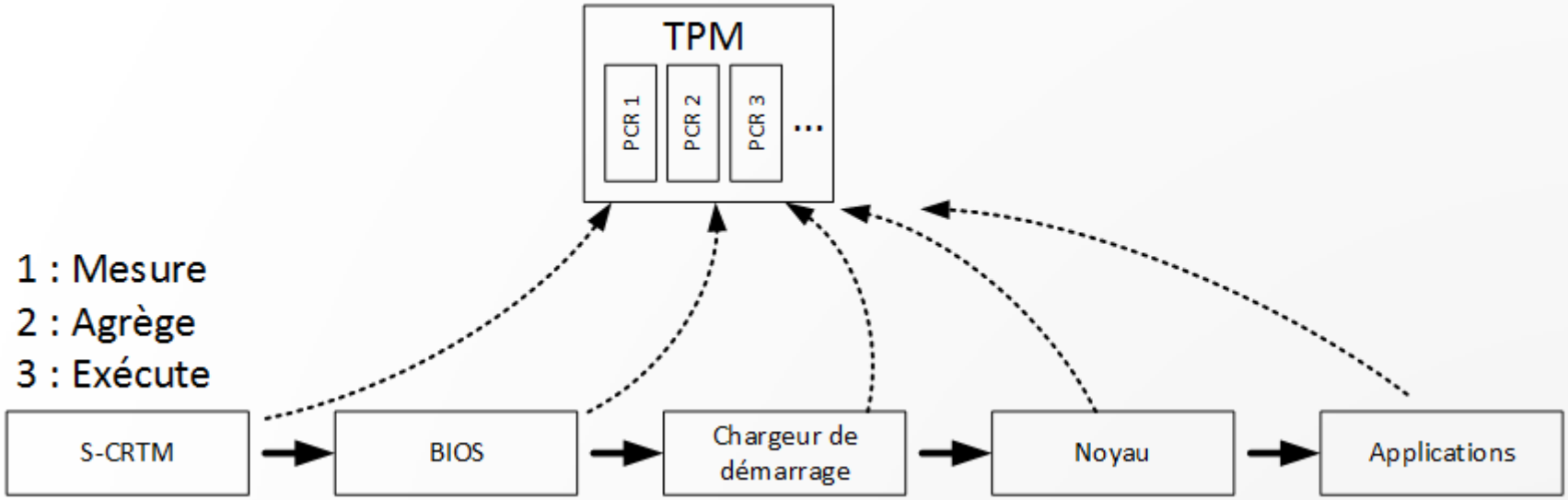

TPM
PCR 1
PCR 2
PCR 3
...
Agrège
Fil d'exécution
Mesure
Chaine de
démarrage

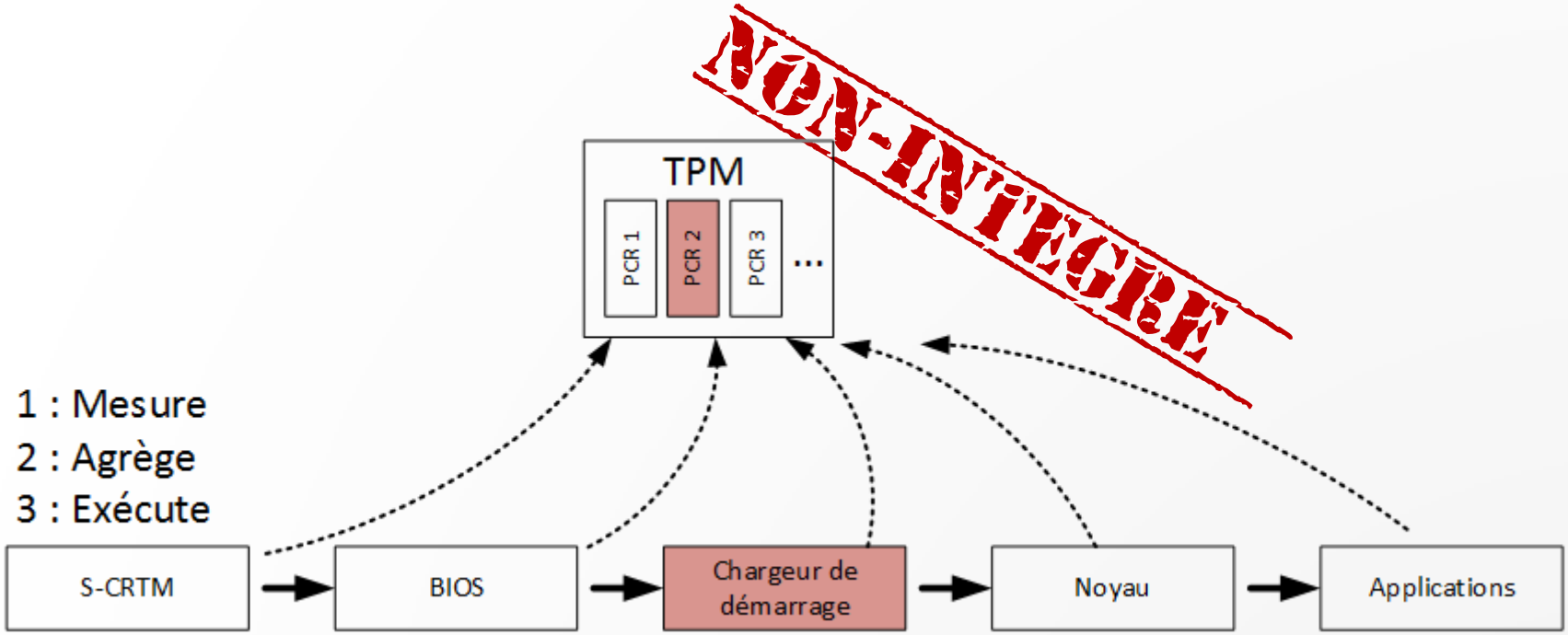

TPM
PCR 1
PCR 2
PCR 3
...
Abstraction deliberée...
Agrège
Fil d'exécution
Mesure
Chaine de démarrage
Pilote noyau
Fichier de configuration

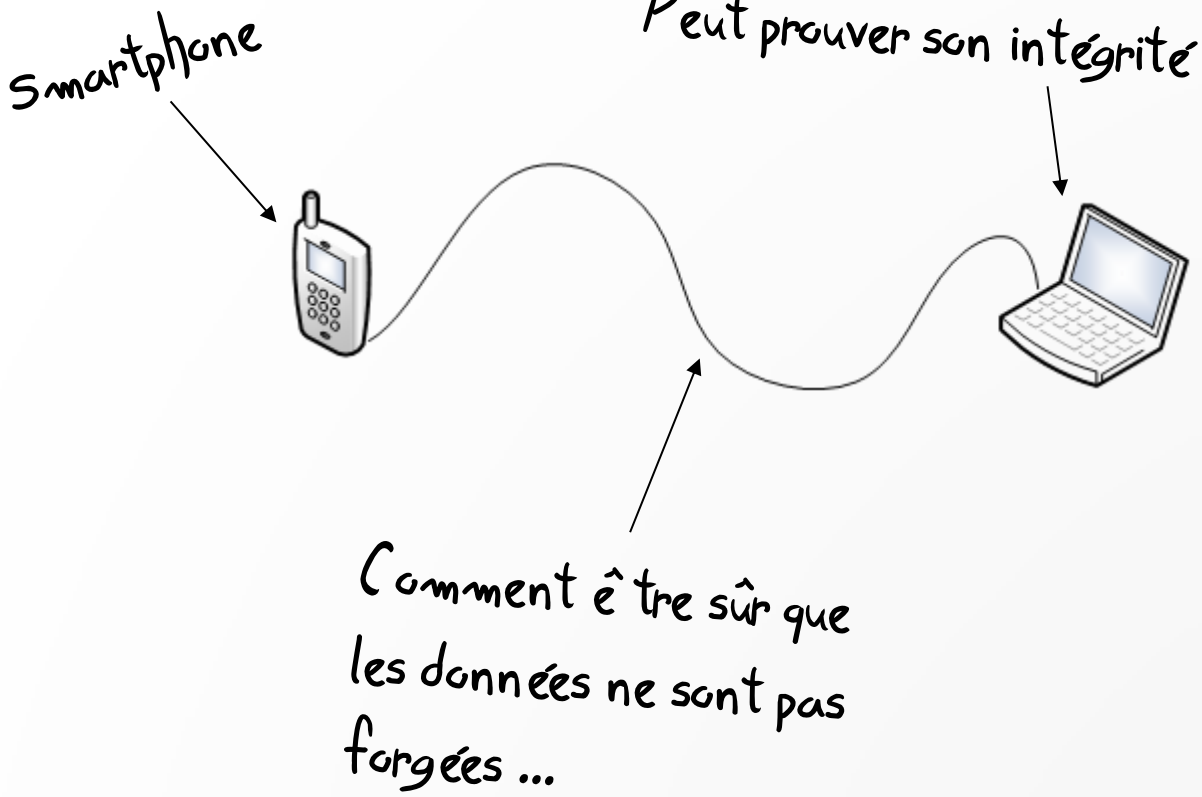
Trust me if you can

- Comment avoir confiance dans le fil d'exécution ?
- Nécessité d'une racine de confiance
- Nécessité d'une chaine de confiance
  - Chaque élément exécuté doit avoir été préalablement mesuré

Exemple d’une chaine de confiance au démarrage

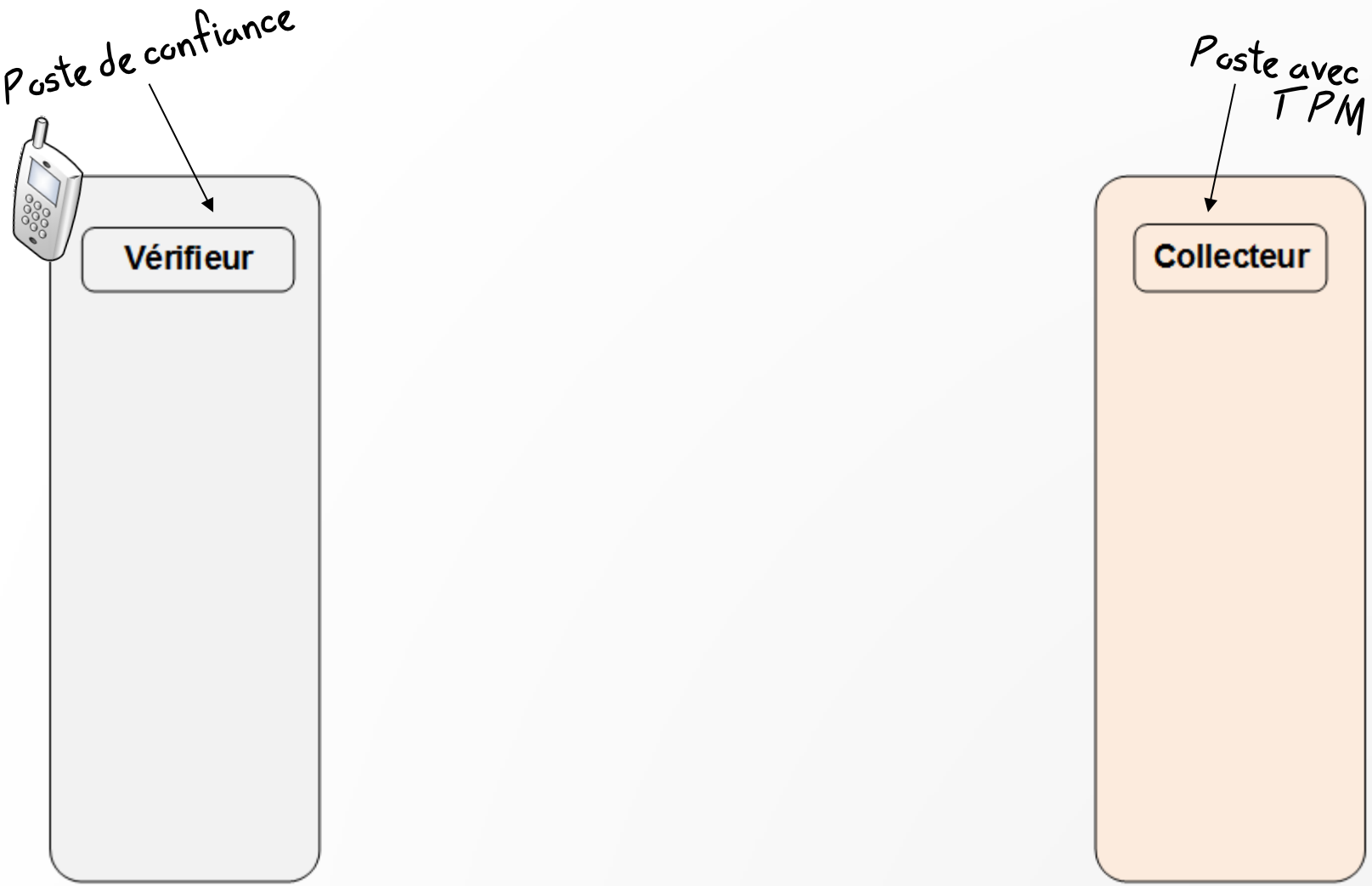

TPM
PCR 1
PCR 2
PCR 3
...
1 : Mesure
2 : Agrège
3 : Exécute
S-CRTM
BIOS
Chargeur de démarrage
Noyau
Applications

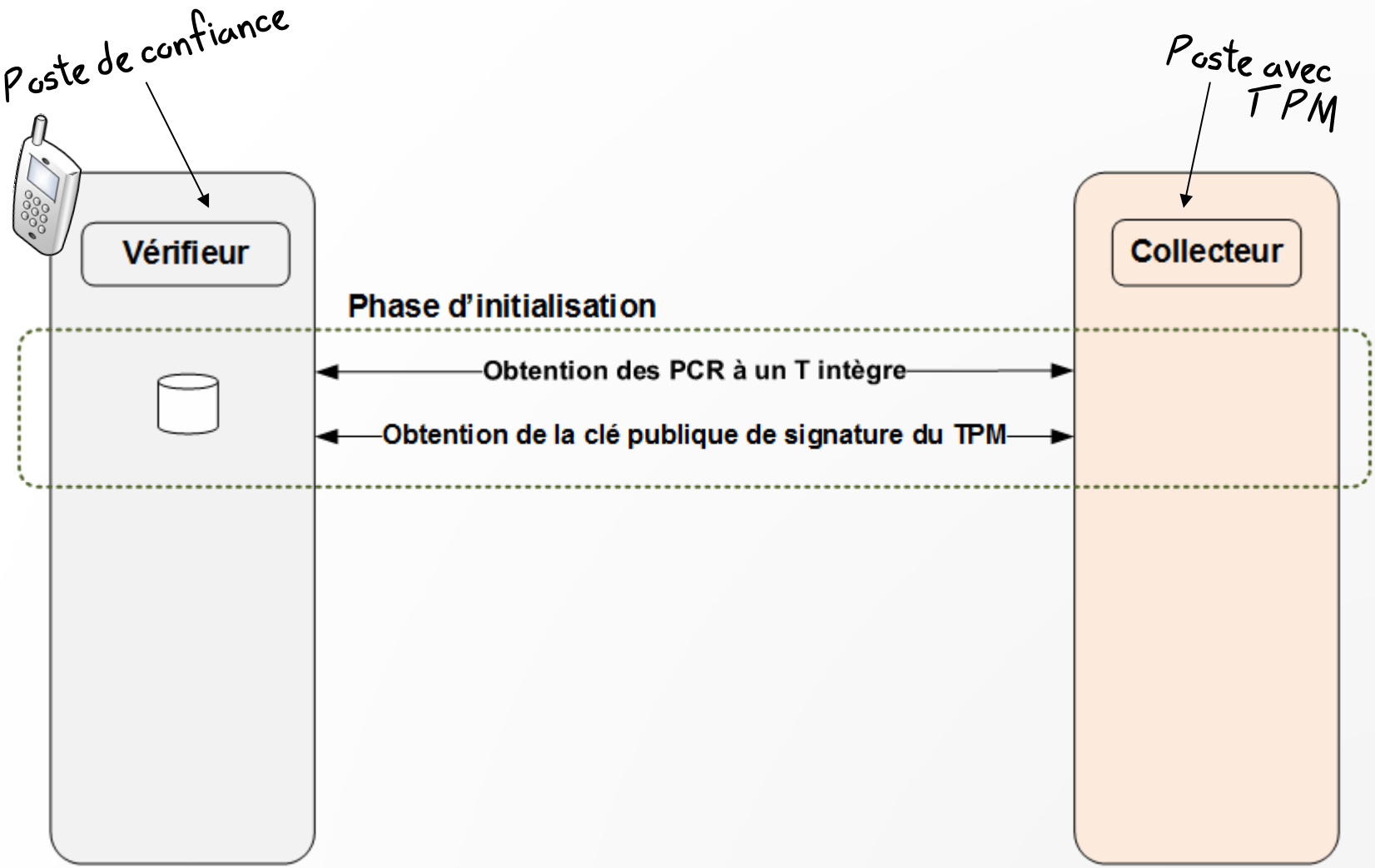

NON-INTEGRE
TPM
PCR 1
PCR 2
PCR 3
...
1 : Mesure
2 : Agrège
3 : Exécute
S-CRTM
BIOS
Chargeur de démarrage
Noyau
Applications

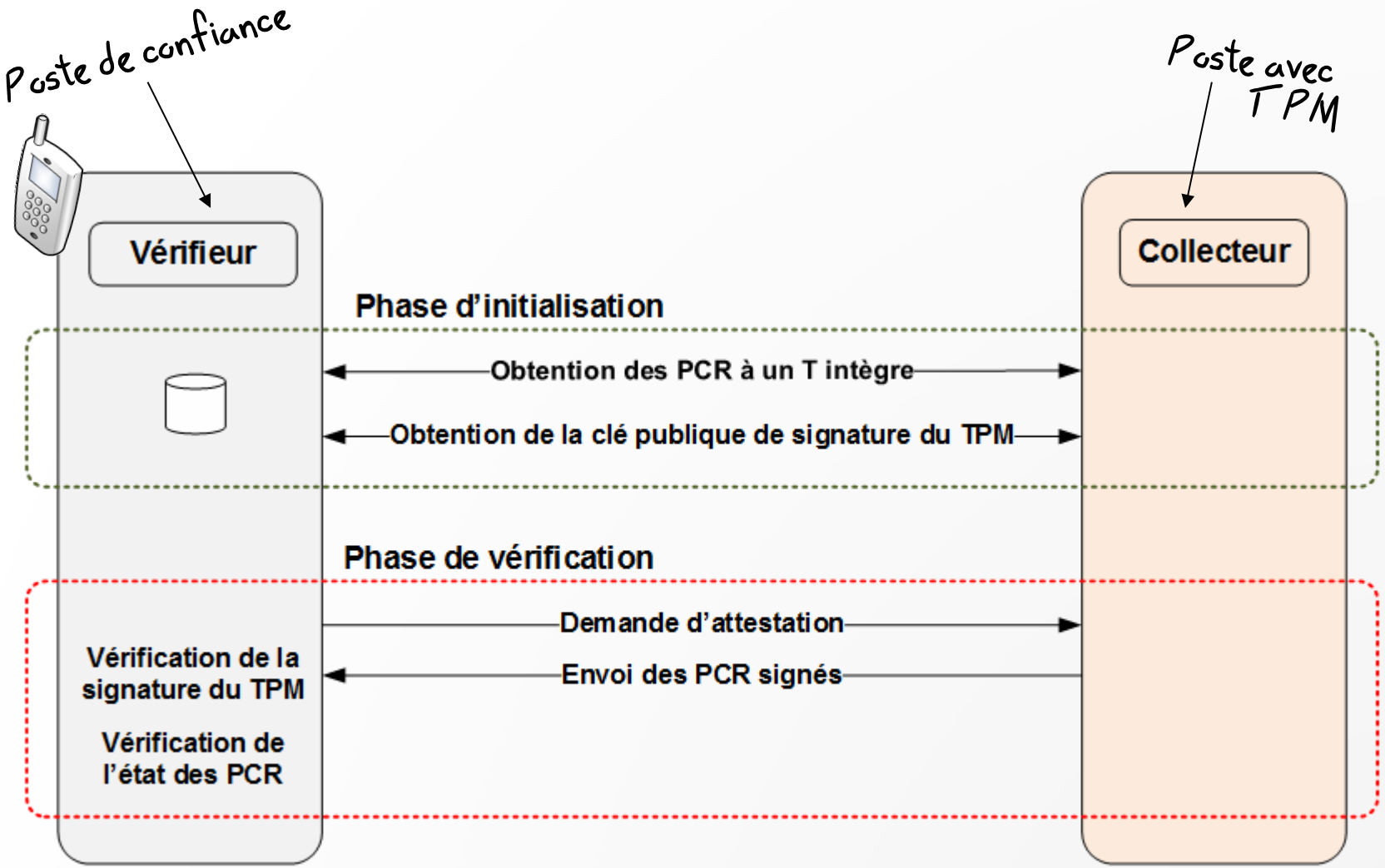

Smartphone
Peut prouver son intégrité
Comment être sûr que
les données ne sont pas
forgées ...

- Utilisation des fonctionnalités de signature du TPM
- Signature des PCR extraits

Cinématique d'une attestation distante

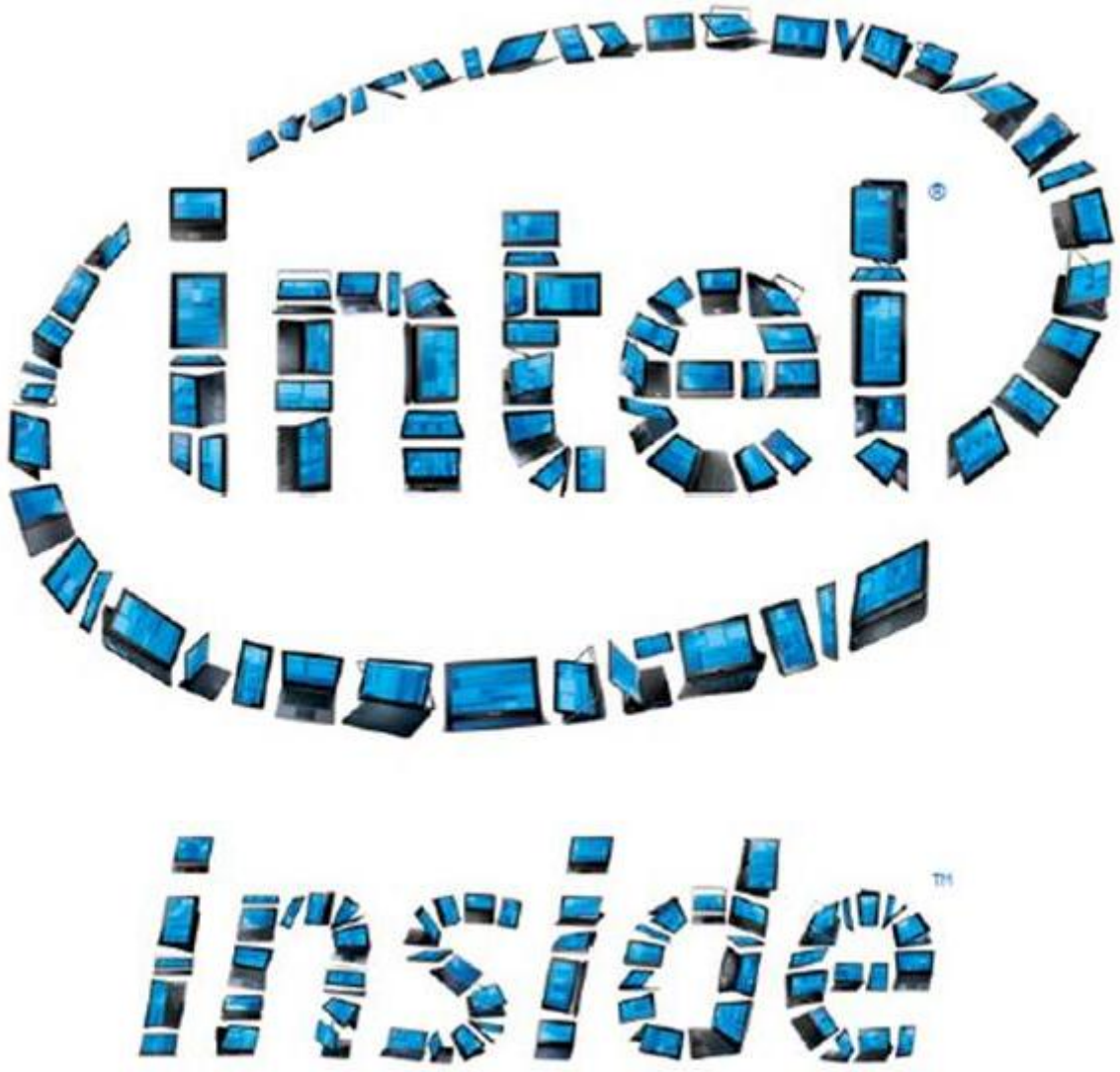

Poste de confiance
Vérifieur
Poste avec TPM
Collecteur


Poste de confiance
Poste avec TPM
Vérifieur
Collecteur
Phase d'initialisation
Obtention des PCR à un T intègre
Obtention de la clé publique de signature du TPM

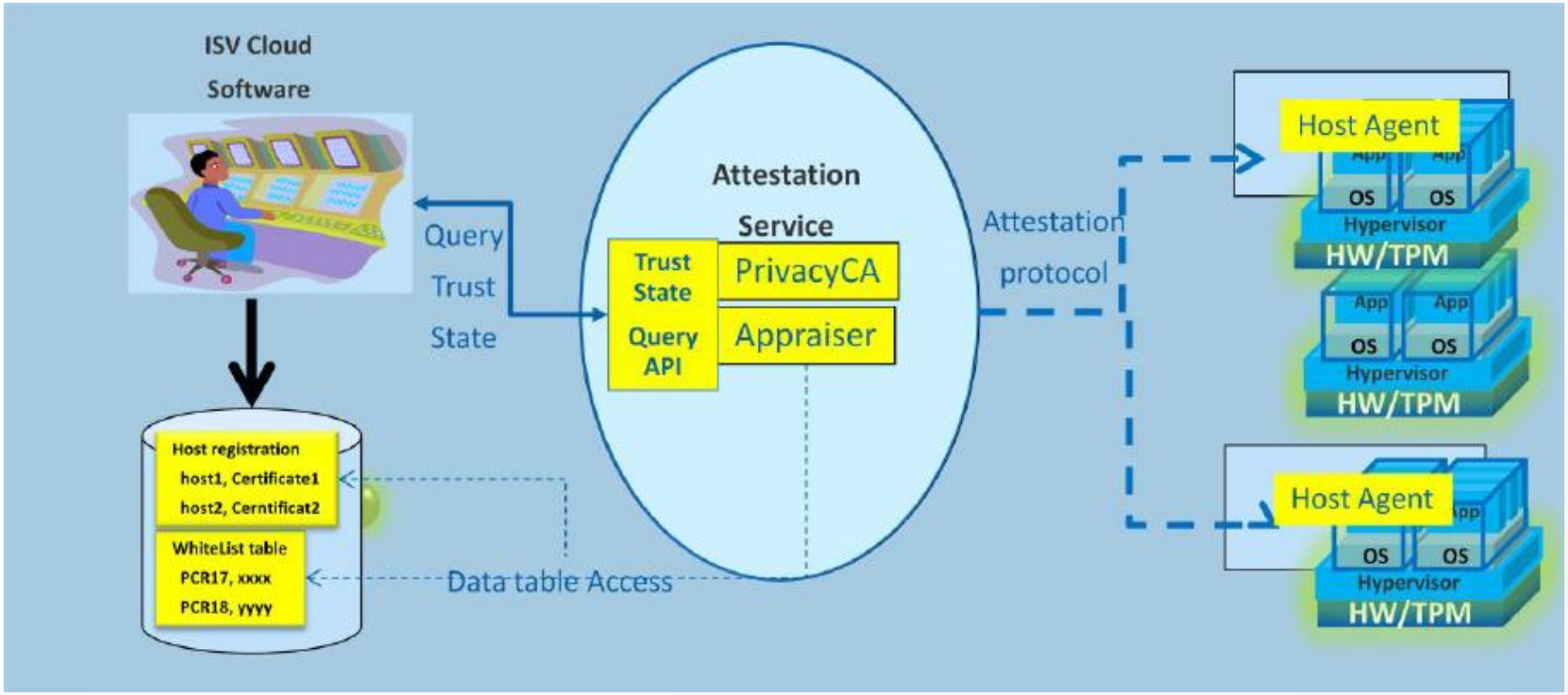

Poste de confiance
Poste avec TPM
Vérifieur
Collecteur
Phase d'initialisation
Obtention des PCR à un T intègre
Obtention de la clé publique de signature du TPM
Phase de vérification
Demande d'attestation
Envoi des PCR signés
Vérification de la signature du TPM
Vérification de l'état des PCR

Théorie

- Quelles implémentations existantes ?
- « OpenAttestation » : Intel
- « OpenPTS » : universitaires japonais


intel
inside

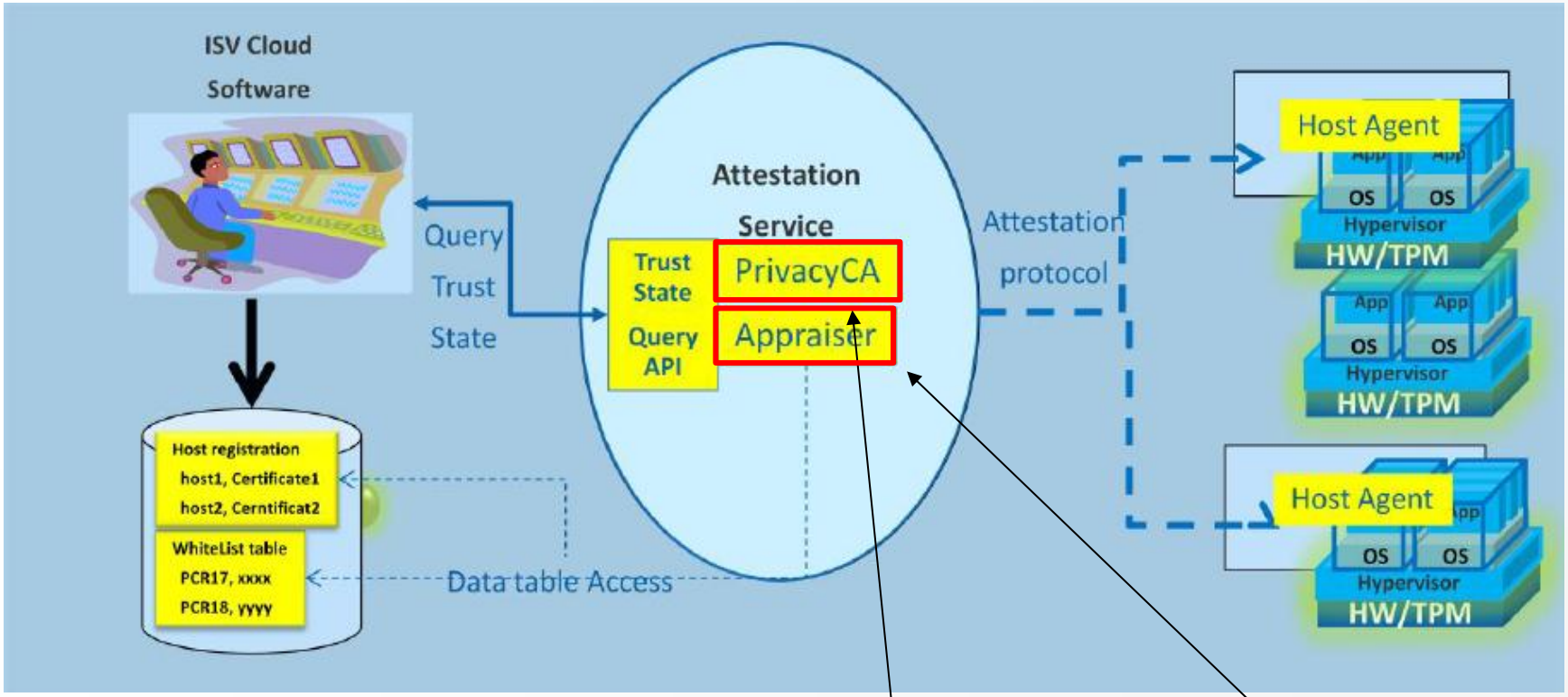
OpenAttestation – By Intel



Source :
OpenAttestation SDK Overview
https://github.com/OpenAttestation/OpenAttestation/blob/master/docs/Overview.pdf

WTF INTEL...

OpenAttestation – By Intel



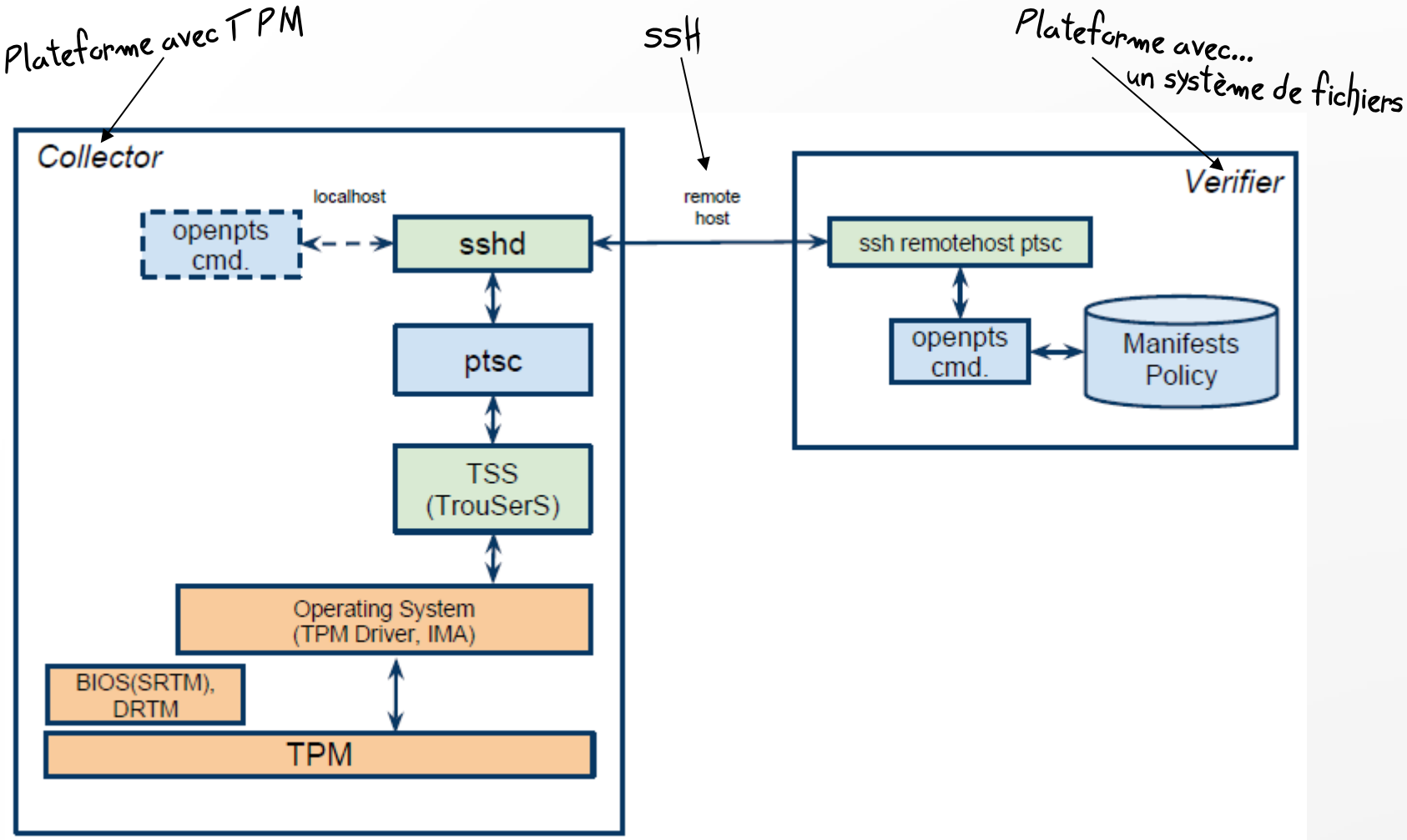
Source :
OpenAttestation SDK Overview
https://github.com/OpenAttestation/OpenAttestation/blob/master/docs/Overview.pdf

OpenAttestation – By Intel

- Utilisation d'une PKI pour vérifier l'identité des TPM
- Embarquer une PKI sur un *smartphone*…

OpenPTS

- (Open) Platform Trust Services
- 2 binaires : un Collecteur, un Vérifieur
- Implémentation de référence du TCG



Source :
Open Platform Trust Services (OpenPTS) User Guide
http://sourceforge.jp/projects/openpts/wiki/!pdf/FrontPage.pdf

OpenPTS

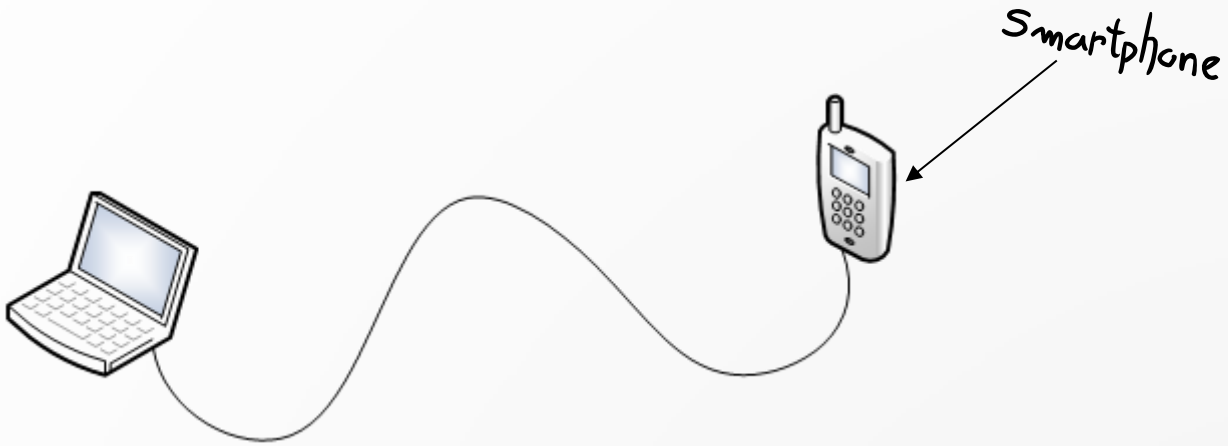
- Version du Vérifieur disponible en Java
- Nécessité d'une connexion SSH


- Press to start tethering. -

USB tethering

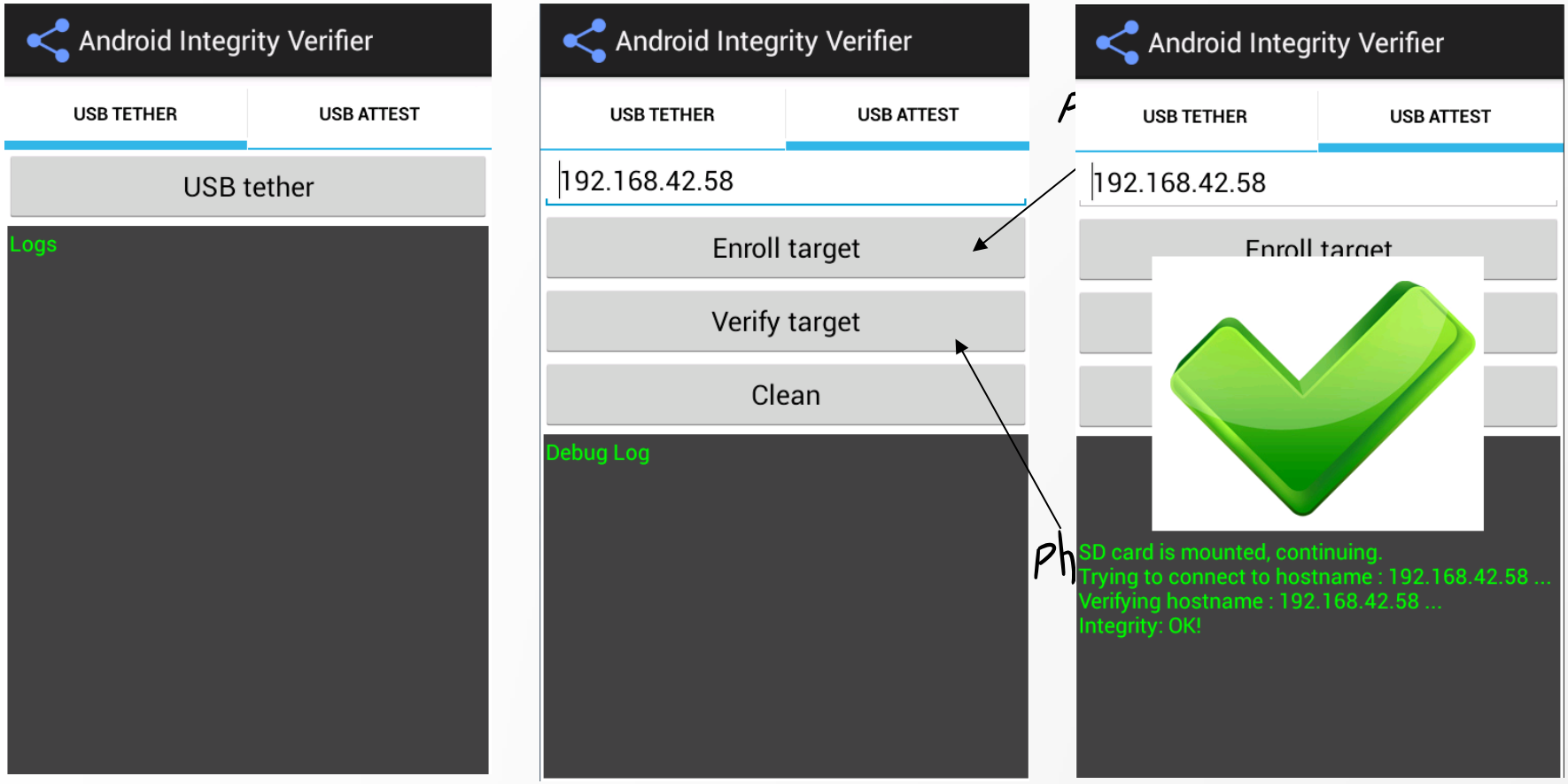
- Permet de partager la connexion réseau du téléphone
- Initialisation d'une interface réseau dédiée

Introducing Android-attest



- DVM == JVM
- SSH over USB

Introducing Android-attest



Cas d'utilisation

- Pendant un déplacement avec des femmes de ménage un peu louches
- Pour des *admins* souhaitant vérifier l'intégrité d'un serveur

Conclusion

- Attester de l'intégrité d'un poste autonome, en basant sa confiance sur son téléphone
- *Plug 'n play* !
- Preuve de concept disponible (bientôt) sous la forme d'un dépôt GitHub

- Développé dans le cadre du projet de recherche OpenDTeX
  - Subventionné par la DGA sous la forme d'un projet RAPID
  - Renforcer la sécurité des postes de travail
  - Implémentant des concepts d'informatique de confiance (boot sécurisé, DRTM, …)

- Questions
- Discussions