

Sécurité des smartphones

D'où on vient
Où on va?

Il y a 20 ans

Carte à Puce bien installée, communications chères et connectivité faible

– Exemples d'applications

- Carte Bancaire



- Risques : n clones 1 carte, → attaque massive avec détection non immédiate → parade : LNoires

- PME : ex MONEO



- SAM → clé de base → n clones d'id quelconque → attaque massive → pas de parade → arrêt du système

– Evaluation sécuritaire

Profil de protection ↔ Cible d'évaluation
Niveau de conformité

} Coûteux

- Ex : EAL4+ :
 - » Hard: Attaques laser, MEB, micropointes...
 - » Soft: conformité aux security requirements de la cible

Évolution des mobiles → smartphones

Mobile=Terminal Internet et support d'applications

OS et langages (JAVA) adaptés mais sécurité?

NFC

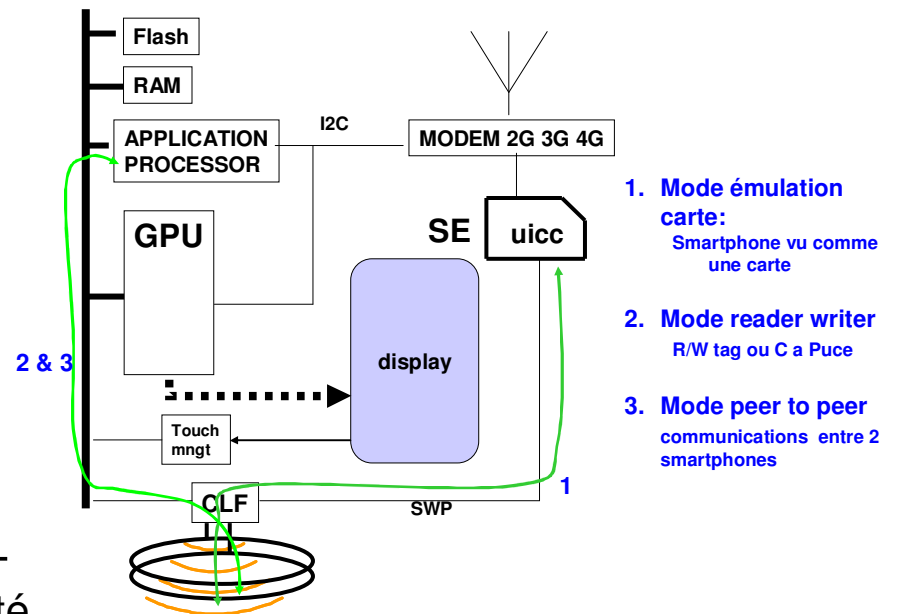
HCE (host card emulation) en 2013

HCE + SE

SE=SIM

SWP, avec SIM évaluées EAL4+

- profil de protection orienté
- isolation applis, authentification forte
- chargement applis et clés
- Normes Global Platform pour les SE



jc.pailles@voila.fr 16/07/2013

Évolution du monde des Télécoms

- Prix en baisse
- Transmission: 3G puis 4G
 - connectivité constante,
 - débits et latence améliorés
- Cloud messaging (ou push)
 - Un serveur reste connecté aux clients
 - Possibilité de collecte de datas (activité, positions...) contrôle, mise à jour des applis

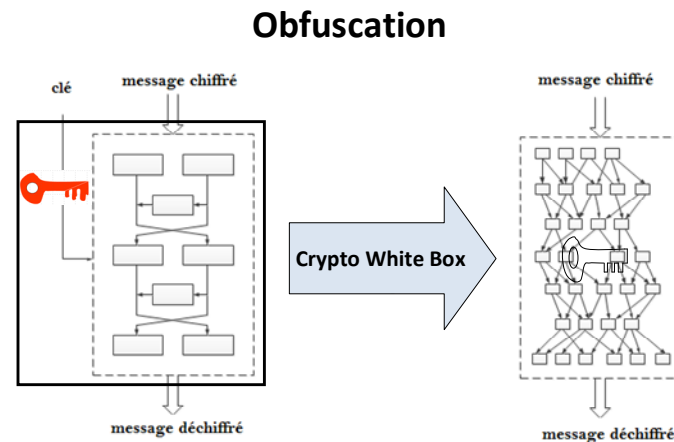
Évolution des applis et leurs moyens de défense

Connectivité → auto-défense dans les applis (au niveau Smartphone et Réseau)

- Multifacteur: 3D secure
- Tokenisation
- Clés à usage limités

} Réduction de la conséquence des attaques

- White Box Crypto
 - Diversifiée?
 - Évolutive?
 - Clonage?
- Révocation facilitée:
 - Ex: changer tous les certificats sauf ceux des fraudeurs
- Monitoring
 - Localisation, usages (fréquence...), etc



Evolution plus récentes smartphones

SIM → eSIM

Approche SIM centric? Sens ?

Généralisation de nouveaux moyens d'authentification utilisateur :
empreintes, visage

Besoin de sécurité plus globale

Il faut sécuriser plus que les clés et data sensibles! Mais on ne peut sécuriser un Smartphone comme une smart-card avec eval sécuritaire

Complexité

Millions de lignes de code comme pour les PCs

Evolutivité

OS et applis

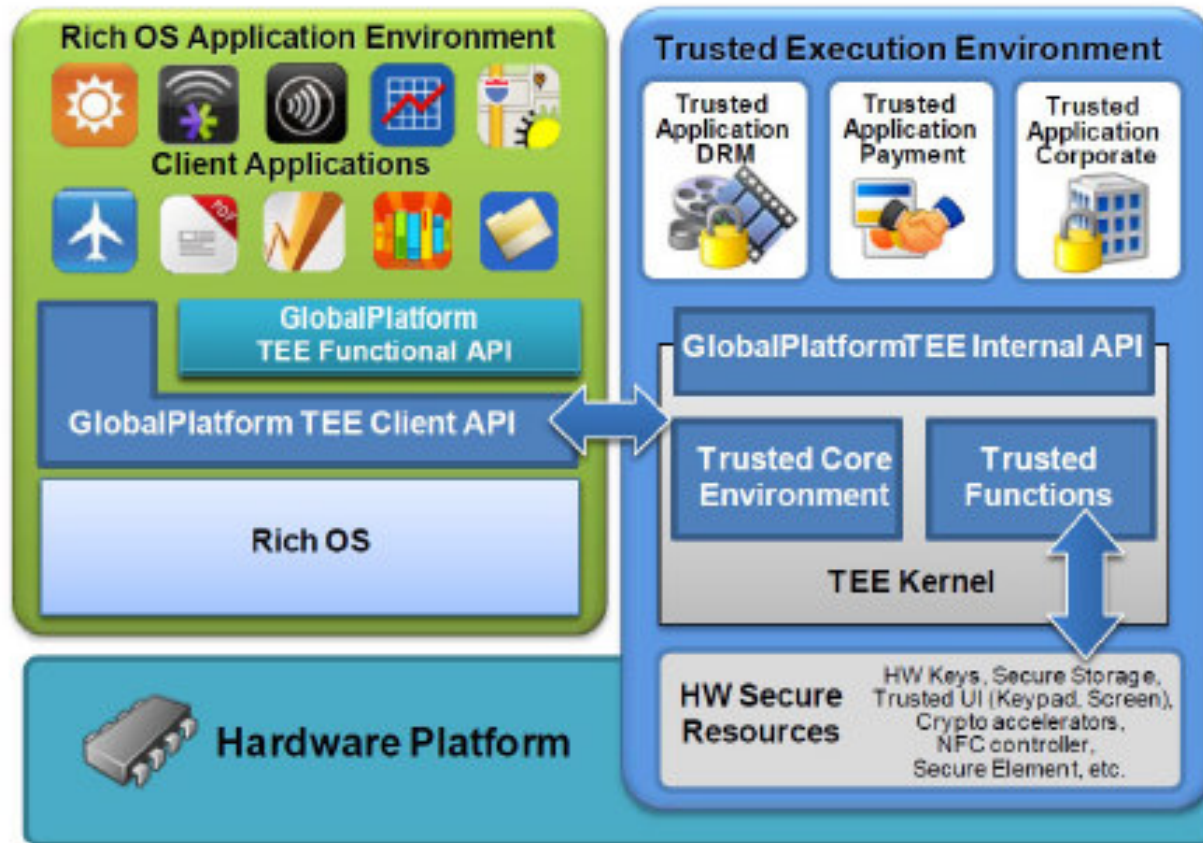
Diversité

1 architecture μ P ARM 7

2 types d'OS mais n versions

couches user spécifiques du vendeur

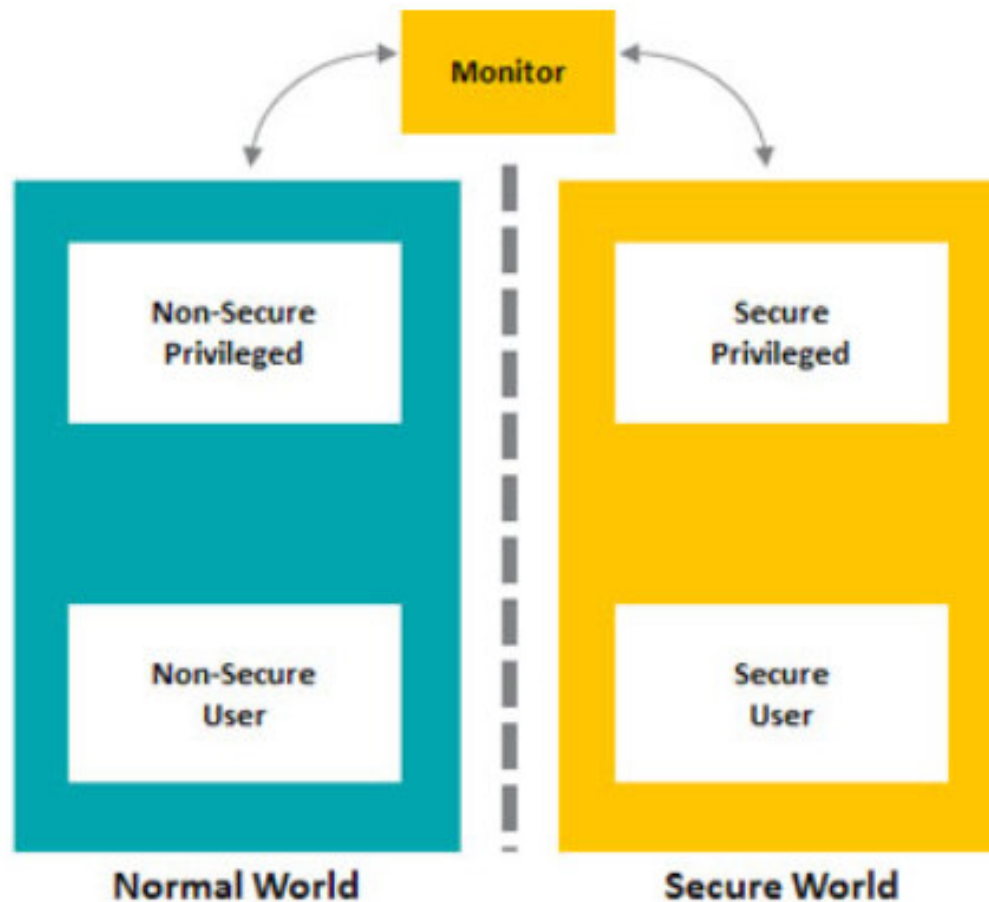
La solution: TEE



Knox de Samsung utilise ce modèle

Comment parvenir à l'approche TEE

Implications au niveau Application Processeur,
Ex: séparer les espaces d'adressage comme avec ARM7

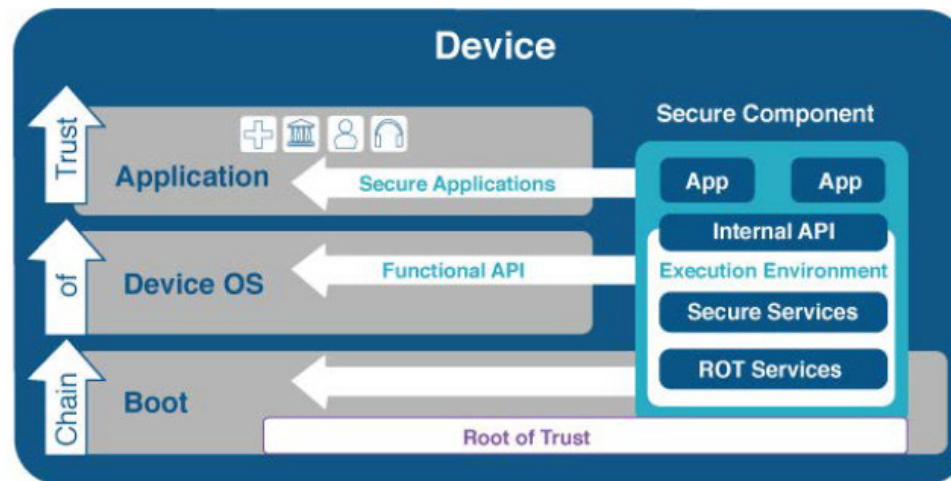


Mais ceci ne suffit pas!

Un OS vit!

- Il est l'assemblage de nombreux programmes d'origine diverses
- Nécessité de mise à jour sécurisées
- A partir d'un bout de code figé: **boot**
- Nécessité d'authentifier l'OS: **attestation**

→ **Root of Trust** (code+ clés figées) **et Secure Boot**



ET en plus:

Comment l'utilisateur peut savoir qu'il est en mode "trusted"?

- Solutions

- Voyant: antiquité!

- Image secrète

- connue de l'utilisateur

Avec conditions:

- Impossible à capter par des applis du rich OS
 - Définie lors de la personnalisation du smartphone

Bref, sujet complexe

- Nécessité d'une standardisation
 - Profils de Protection
- Adhésion des fabricants de Smartphone
- Infrastructure de certification
 - Labos d'évaluation
 - Certification des labos
 - Architecture du smartphone
 - Phase personnalisation
 - Infrastructure non monopolistique: Trustonic?
- Portabilité des softs sécurisés
 - Applets, Trustlets

Global Platform

<https://globalplatform.org/>

The GlobalPlatform TEE Management Framework

The document defines standard methods to manage the lifecycle of the TEE once it is active. In order to support the variety of usage of the TEE in today's digital world, the document supports a number of deployment models, including: one or many actors; connected or unconnected devices; and one-to-one or one-to-many devices, as well as with symmetric and asymmetric cryptography.

[Download the framework](#)

GlobalPlatform TEE Protection Profile

Certified against Common Criteria under its Trusted Computing category, this document specifies the typical threats the hardware and software of the TEE needs to withstand. It also details the security objectives that are to be met in order to counter these threats and the security functional requirements that a TEE will have to comply with.

[Download the TEE Protection Profile](#)

TEE Compliant Products

GlobalPlatform has developed an open and thoroughly evaluated TEE ecosystem with accredited laboratories and certified products.

The GlobalPlatform TEE Certification Scheme, managed by its TEE Security Evaluation Secretariat, enables vendors to confirm conformance of their TEE products to the organization's **TEE Protection Profile**, through independent security evaluation.

[View certified products available to purchase](#)

Personnes à contacter:
Christophe Colas, Trustonic
Gil Bernabeu, Gemalto

Où on va?

Plusieurs scénarios envisageables?

- **Succès de l'approche évaluation TEE/GP**
 - Adhésion des fabricants
 - Les prestataires ont confiance en les évaluations
 - Applis auto-sécurisées, et monitoring on-line
 - Surcoûts d'évaluation

- **Echec de l'approche évaluation TEE/GP**
 - Les fabricants ont tous des solutions maison
 - Les prestataires ont confiance en leur notoriété
 - Applis auto-sécurisées, et monitoring on-line

Mais

 - risque de désintermédiation pour les prestataires
 - Surcoûts : non portabilité des applis entre les solutions maison!