Des environnements sécurisés indépendants rarement libres dans vos systèmes

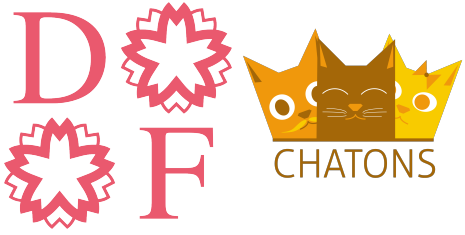
Vincent Giraud

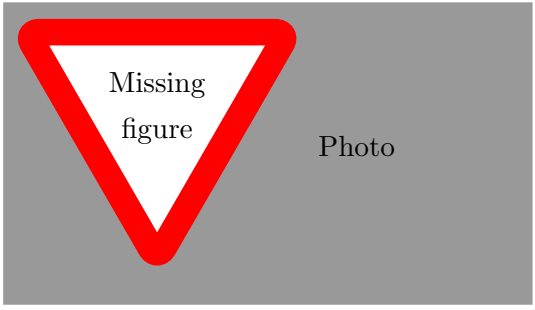
Samedi 16 novembre 2024

Vincent Giraud

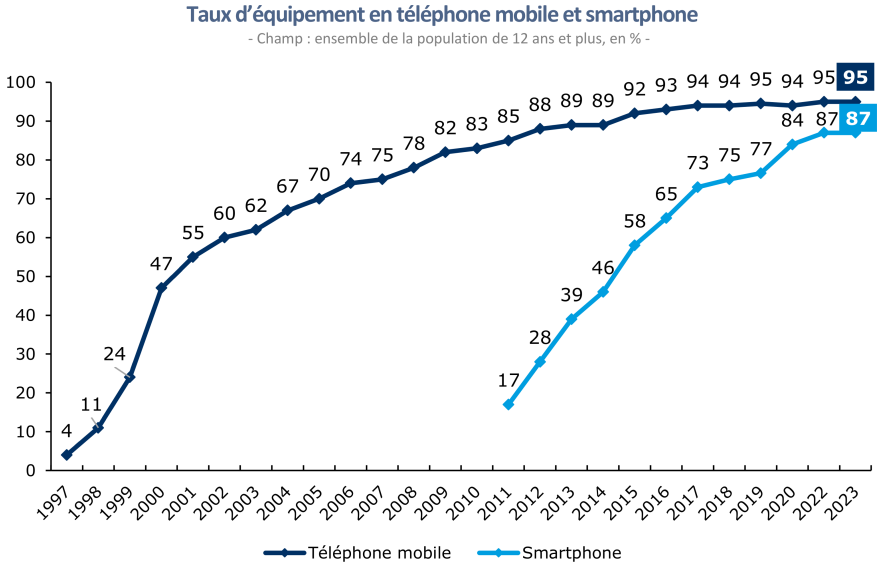
Chercheur en sécurité informatique

Membre de Deuxfleurs





Contexte



CRÉDOC, *Baromètre du numérique*, 2023.

*La définition admise par tous est qu'un COTS (*Commercial Off The Shelf*) est un composant issu du marché ou plus communément appelé un composant sur étagère.*

Philippe Roose. *SI-COTS : Aide à l'intégration de COTS Products*, 2009.

A general-purpose mobile computing device (e.g., smartphone or tablet) that is not designed solely for the purposes of payment acceptance.

PCI Security Standards Council. *Mobile Payments on COTS*, 2023.

- Communications sécurisées

- Communications sécurisées
- Stockage sécurisé

- Communications sécurisées
- Stockage sécurisé
- Biométrie

- Communications sécurisées
- Stockage sécurisé
- Biométrie
- Authentification

- Communications sécurisées
- Stockage sécurisé
- Biométrie
- Authentification

WebAuthn

- Communications sécurisées
- Stockage sécurisé
- Biométrie
- Authentification
- Transport

- Communications sécurisées
- Stockage sécurisé
- Biométrie
- Authentification
- Transport
- Paiement

SAMSUNG
Pay

Embedded microprocessor applications all share one common trait : the end product is not a computer. The user may not realize that a computer is included (...). The teenager watching MTV is unaware that embedded computers control the cable box and the television. (...)
For the purpose of this book, an embedded system is any application where a dedicated computer is built right into the system.

Jack G. Ganssle. *The Art of Programming Embedded Systems*, 1991.

Embedded systems are computing systems dedicated to specific tasks. In many cases, the work being done was originally done by custom logic.

Alfredo Romagosa. *Embedded Systems Journal : Cache Coherence Issues for Real-Time Multiprocessing*, 1997.

Un système embarqué est un système informatique logiciel et matériel enfoui dans un objet afin de contrôler son activité et sa sécurité, d'offrir des services à ses utilisateurs et de communiquer avec d'autres objets.

Gérard Berry. *Pourquoi et comment le monde devient numérique*, 2008.

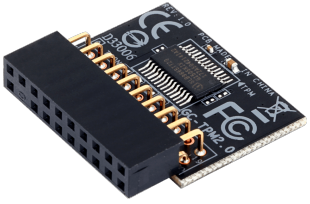
Un objet communicant permet à l'utilisateur d'accéder à des services via cet objet grâce à un échange d'informations avec le monde qui l'entoure.
Les dispositifs numériques qui permettent d'offrir ces services sont appelés systèmes embarqués.

Didier Hallépée. *La sécurité du smartphone et des systèmes embarqués*, 2012.

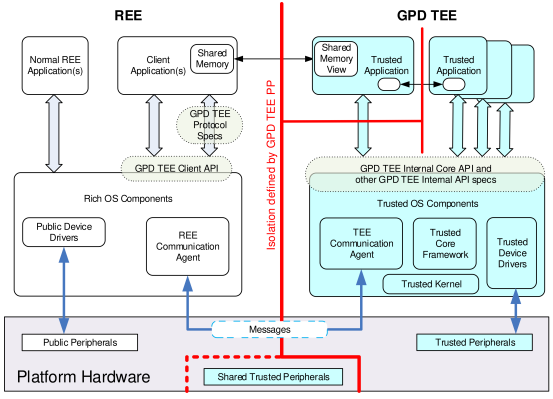
Hardware Security Modules (HSM)

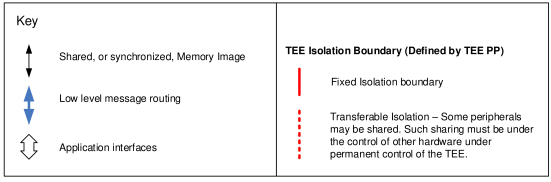
Secure Elements (SE)

Trusted Platform Modules (TPM)

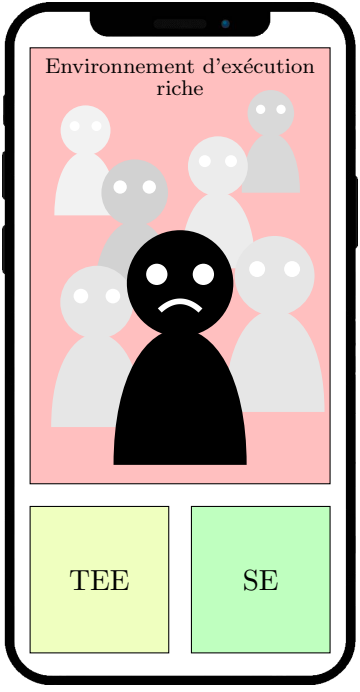


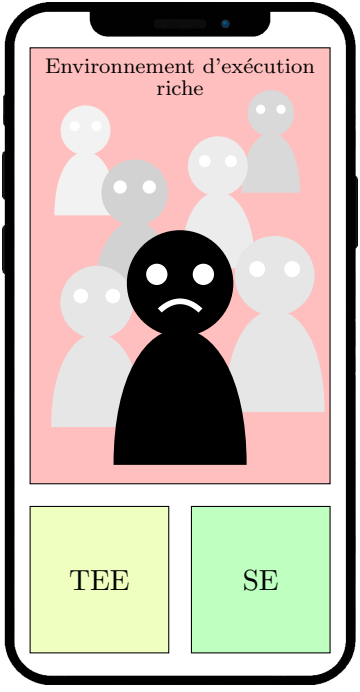
Trusted Execution Environments (TEE)

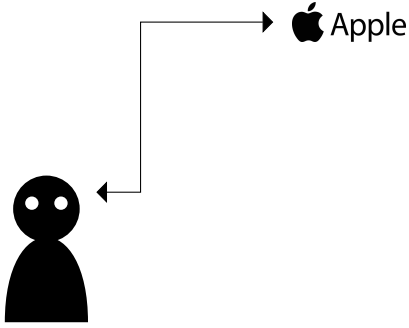


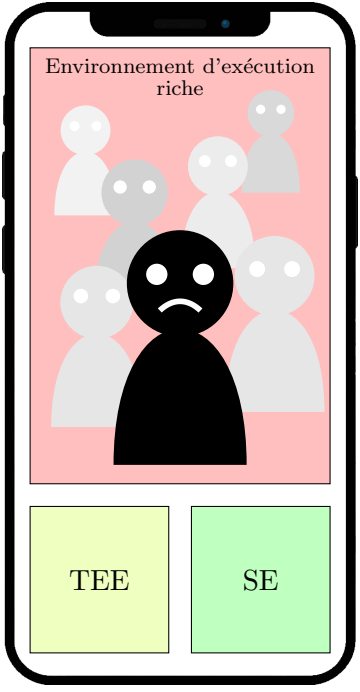


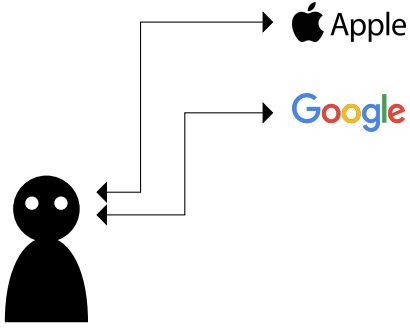
GlobalPlatform, Inc. *TEE Protection Profile*, 2020.

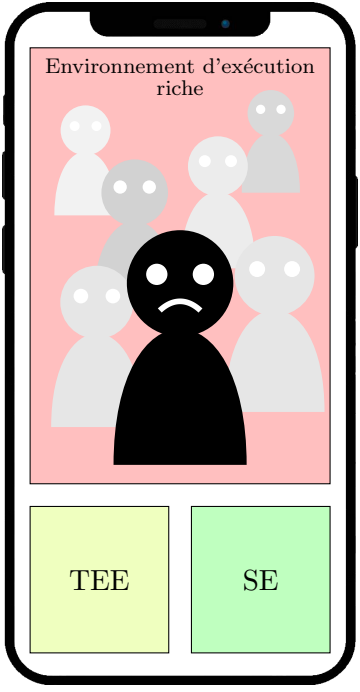

Environnement d'exécution riche
TEE
SE

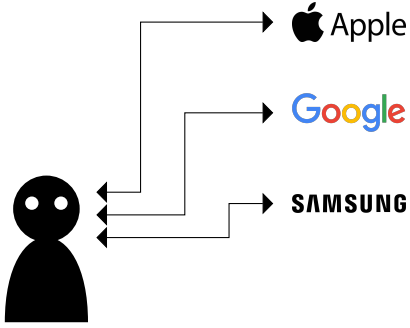

Environnement d'exécution riche
TEE
SE

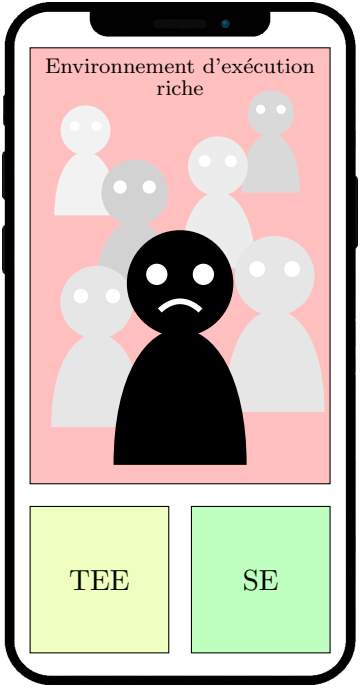

Apple

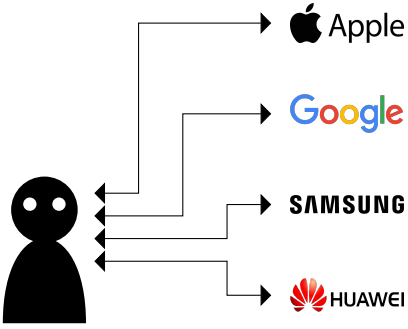

Environnement d'exécution riche
TEE
SE

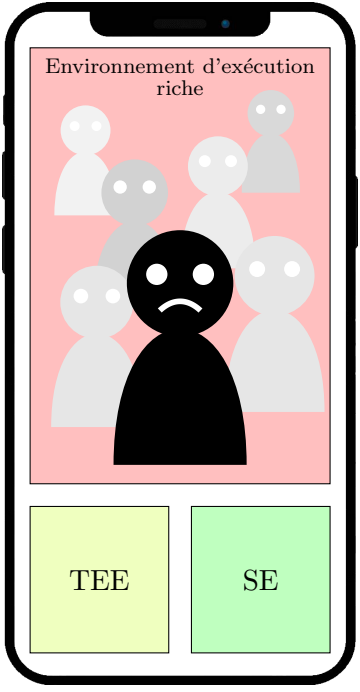

Apple
Google

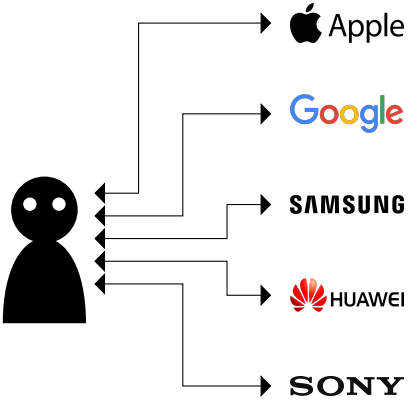

Environnement d'exécution riche
TEE
SE

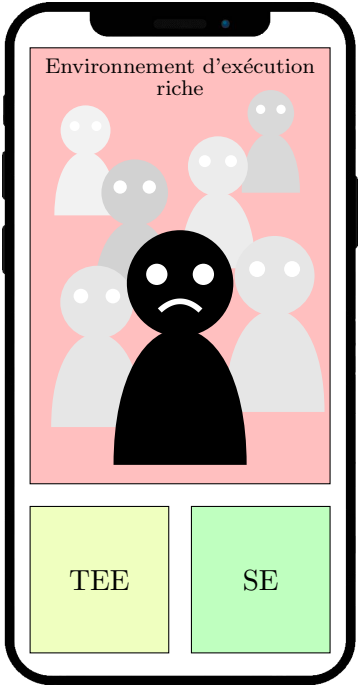

Apple
Google
SAMSUNG

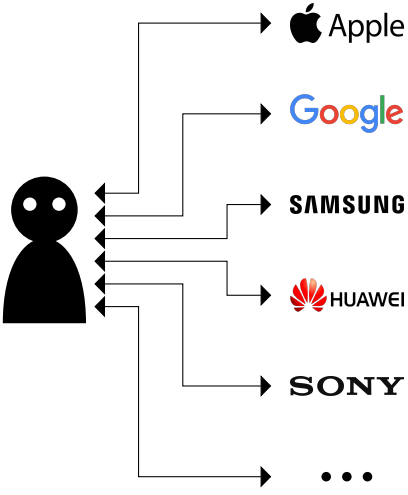

Environnement d'exécution riche
TEE
SE


Apple
Google
SAMSUNG
HUAWEI

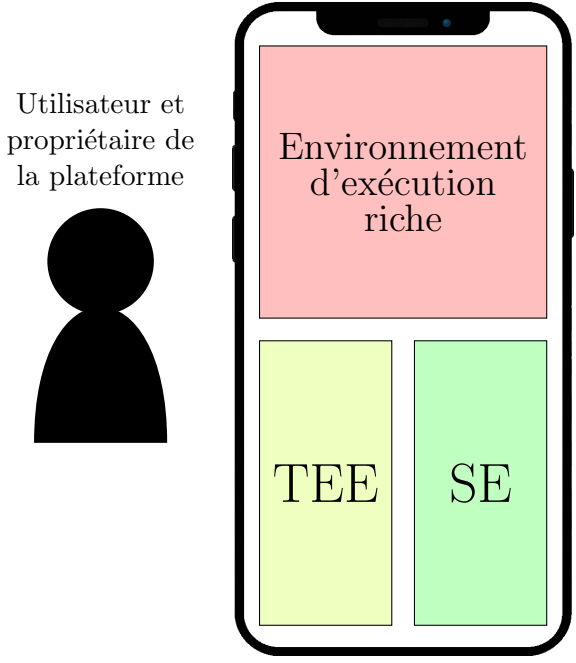

Environnement d'exécution riche
TEE
SE


Apple
Google
SAMSUNG
HUAWEI
SONY

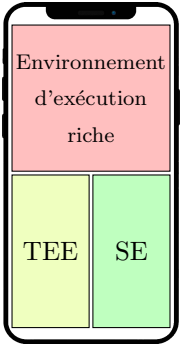

Environnement d'exécution riche
TEE
SE


Apple
Google
SAMSUNG
HUAWEI
SONY
• • •

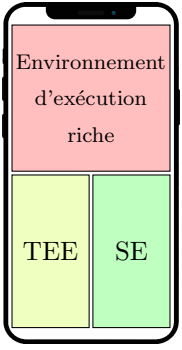
Propositions


Utilisateur et propriétaire de la plateforme
Environnement d'exécution riche
TEE
SE

Utilisateur et propriétaire de la plateforme



Utilisateur et propriétaire de la plateforme

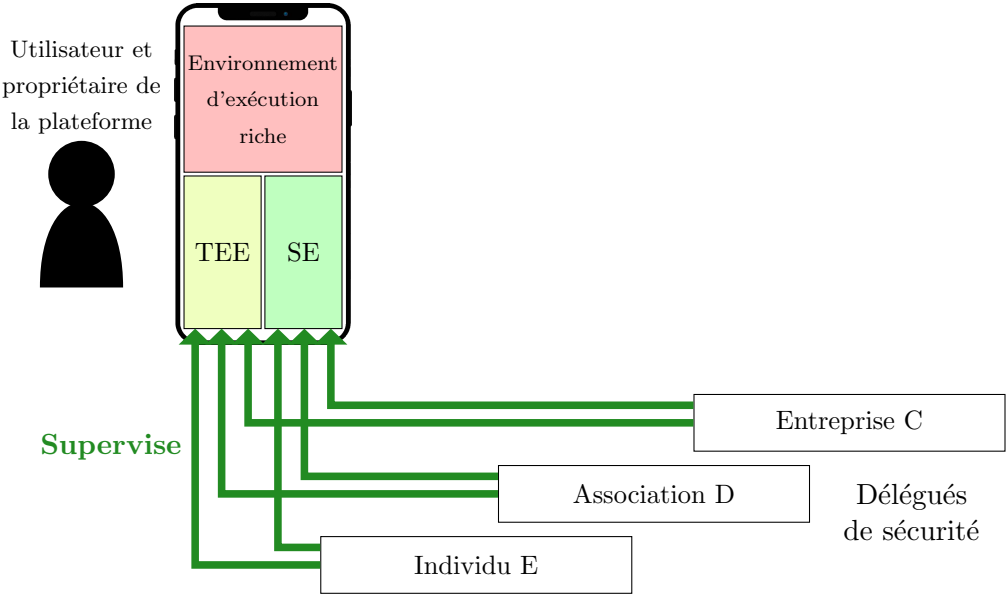


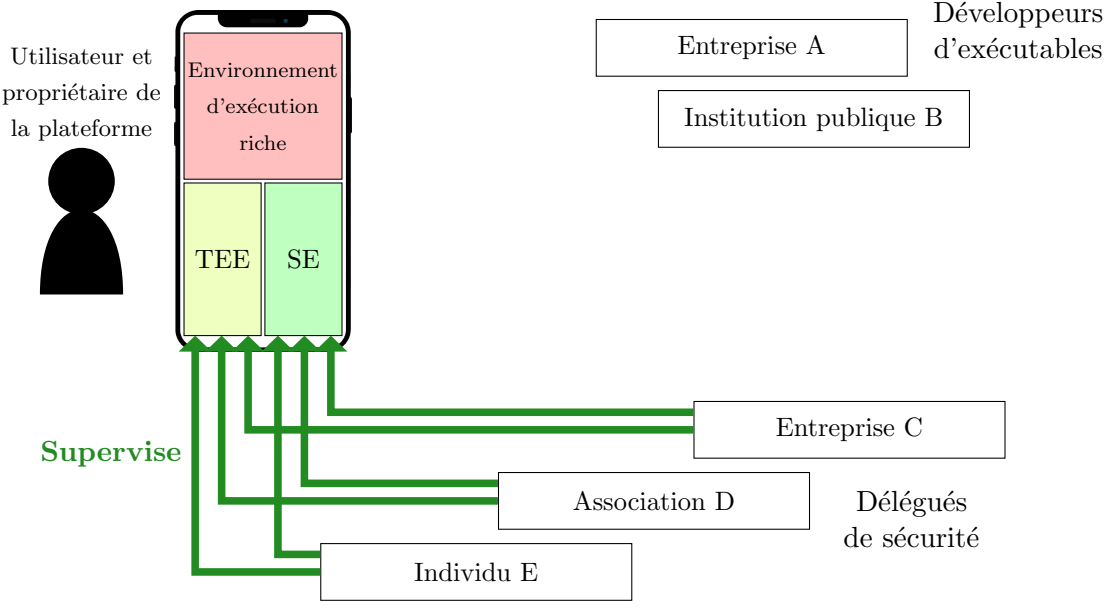
Entreprise C

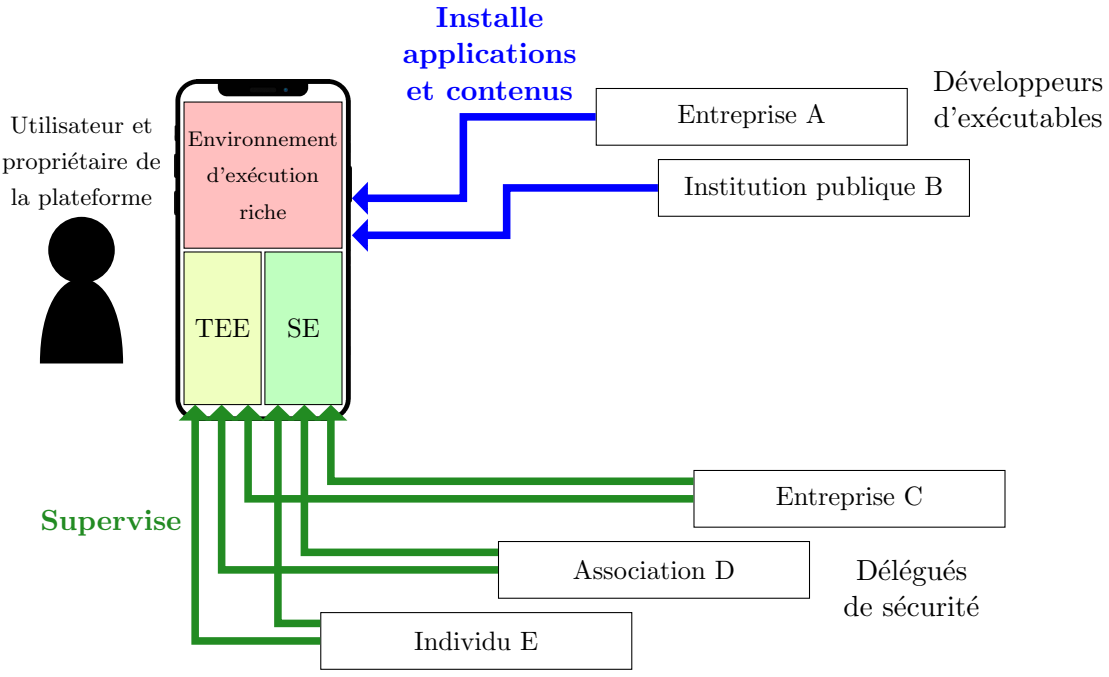
Association D

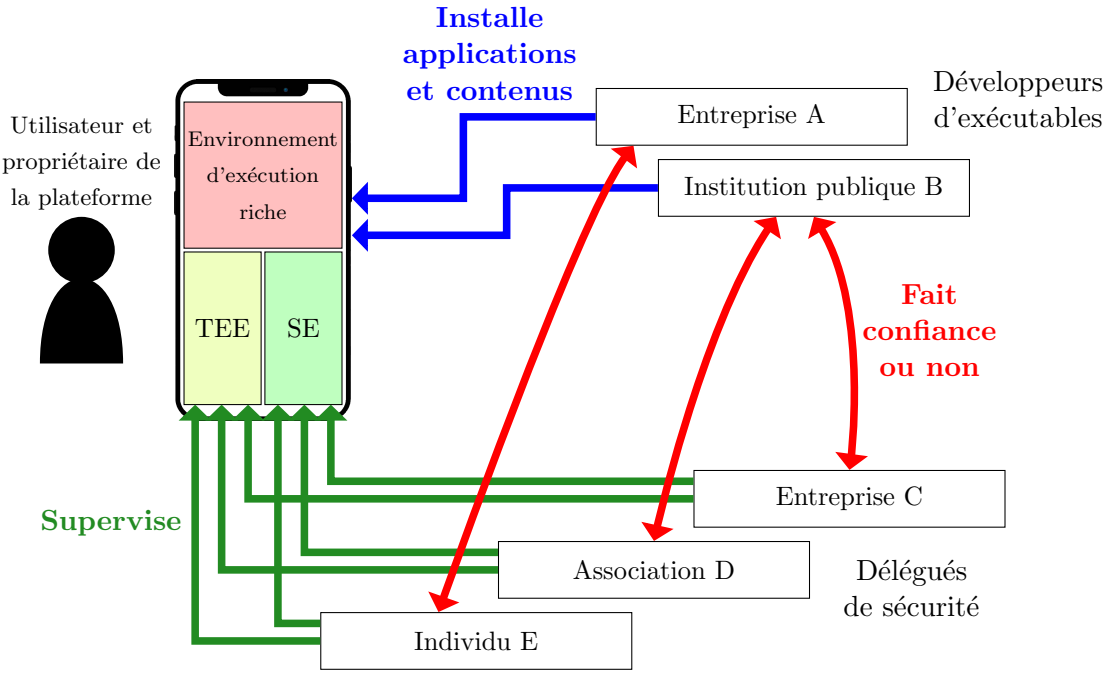
Individu E

Délégués de sécurité


Utilisateur et propriétaire de la plateforme
Environnement d'exécution riche
TEE
SE
Supervise
Entreprise C
Association D
Individu E
Délégués de sécurité


Utilisateur et propriétaire de la plateforme
Environnement d'exécution riche
TEE
SE
Développeurs d'exécutables
Entreprise A
Institution publique B
Supervise
Entreprise C
Association D
Délégués de sécurité
Individu E


Installe
applications
et contenus
Développeurs
d'exécutables
Entreprise A
Institution publique B
Utilisateur et
propriétaire de
la plateforme
Environnement
d'exécution
riche
TEE
SE
Supervise
Entreprise C
Association D
Délégués
de sécurité
Individu E


Installe applications et contenus
Développeurs d'exécutables
Utilisateur et propriétaire de la plateforme
Environnement d'exécution riche
TEE
SE
Entreprise A
Institution publique B
Fait confiance ou non
Supervise
Entreprise C
Association D
Délégués de sécurité
Individu E

Constructeurs de composants sécurisés

Délégués de sécurité

Entreprise C

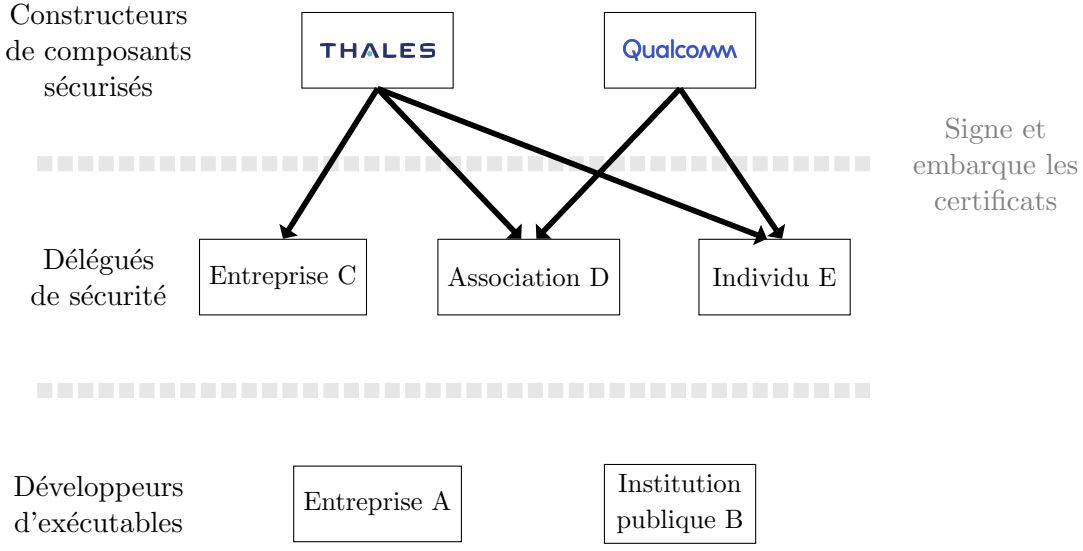
Association D

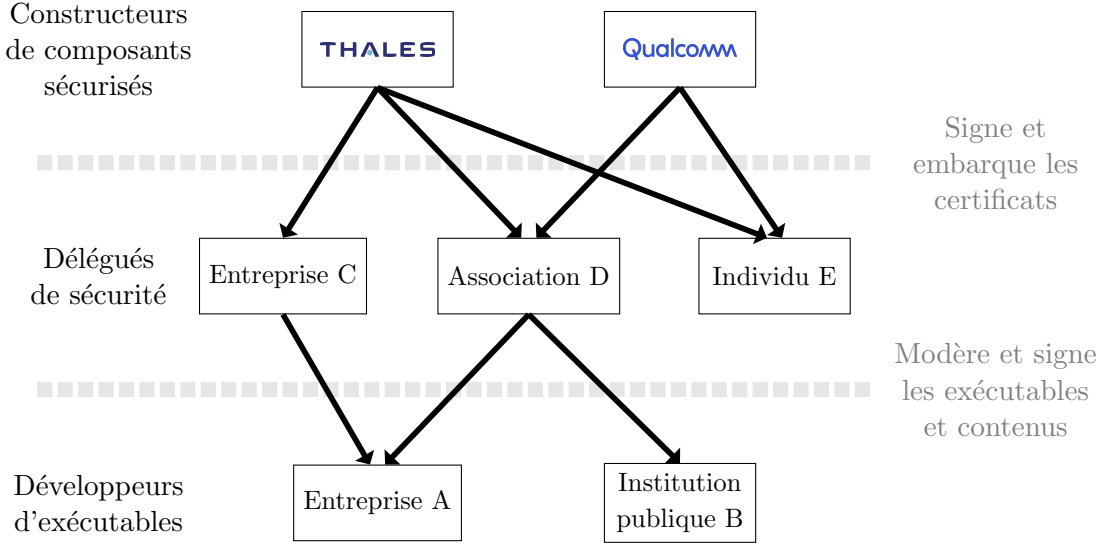
Individu E

Développeurs d'exécutables

Entreprise A

Institution publique B


Constructeurs de composants sécurisés
THALES
Qualcomm
Signe et embarque les certificats
Délégués de sécurité
Entreprise C
Association D
Individu E
Développeurs d'exécutables
Entreprise A
Institution publique B


Constructeurs de composants sécurisés
THALES
Qualcomm
Signe et embarque les certificats
Délégués de sécurité
Entreprise C
Association D
Individu E
Modère et signe les exécutables et contenus
Développeurs d'exécutables
Entreprise A
Institution publique B

Constructeurs
de cor
séc

ne et
rque les
ificats

Dé
de s

e et signe
cutables
ntenus

Déve
d'exécutables

publique B