Des environnements sécurisés indépendants rarement libres dans vos systèmes

Capitole du Libre 2024

Samedi 16 novembre 2024

Vincent Giraud

Chercheur en sécurité informatique

Membre de Deuxfleurs

Comptoir National d'Escompte de Paris, à Angers
Rue Chaussée St-Pierre - L. V., phot.

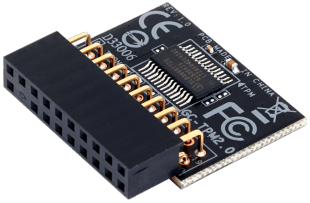
Hardware Security Modules (HSM)

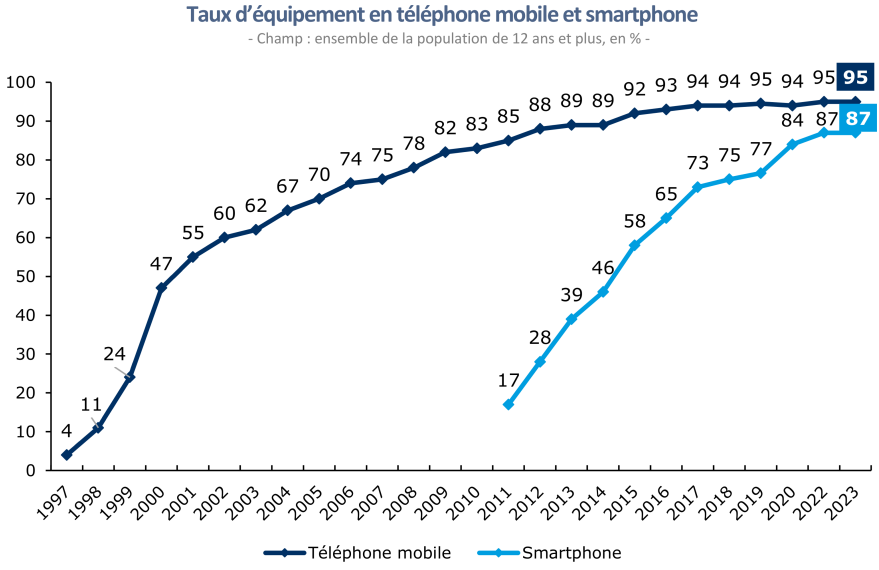
Hardware Security Modules (HSM)

Secure Elements (SE)

Secure Elements (SE)

Trusted Platform Modules (TPM)





CRÉDOC, *Baromètre du numérique*, 2023.

- Communications sécurisées

- Communications sécurisées
- Stockage sécurisé

- Communications sécurisées
- Stockage sécurisé
- Biométrie

- Communications sécurisées
- Stockage sécurisé
- Biométrie
- Authentification

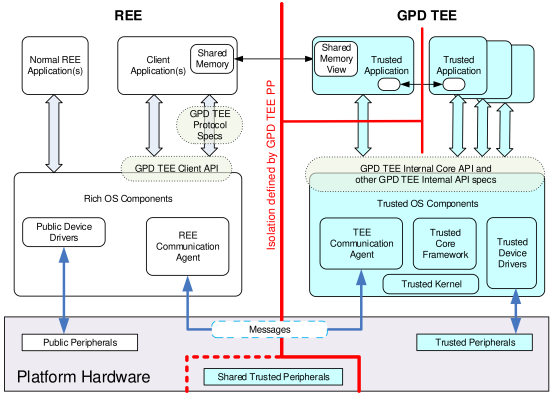
- Communications sécurisées
- Stockage sécurisé
- Biométrie
- Authentification

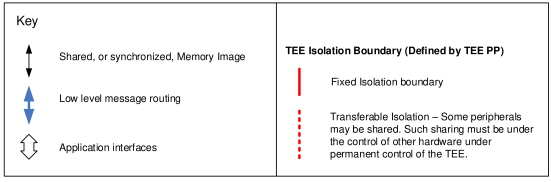
WebAuthn

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

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

Trusted Execution Environments (TEE)

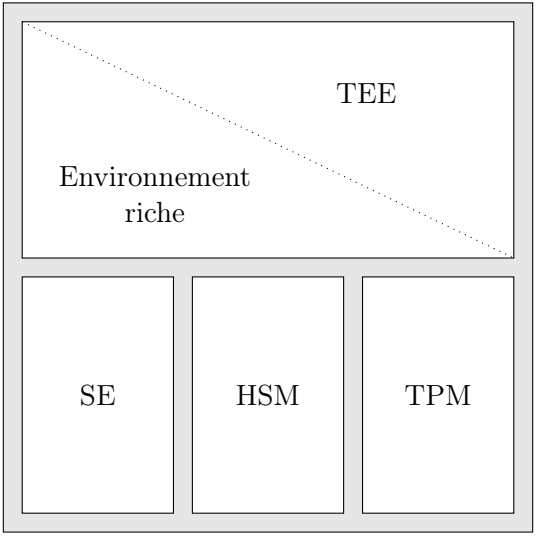


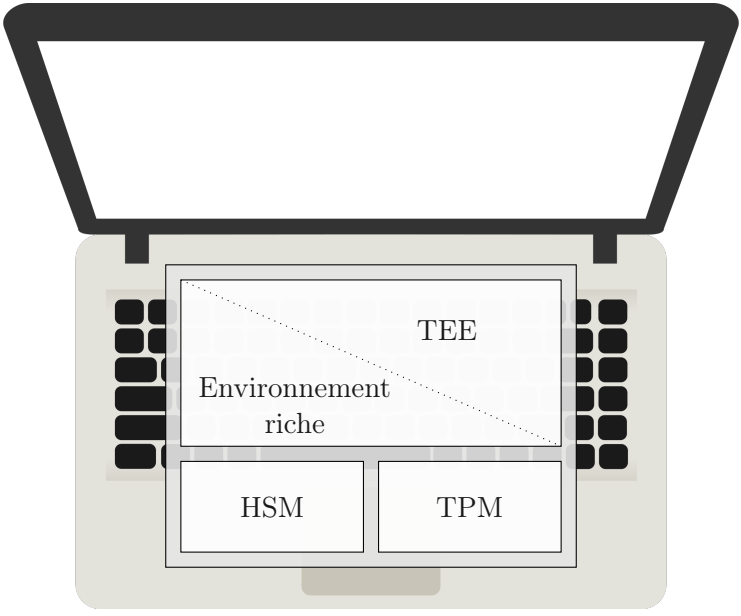


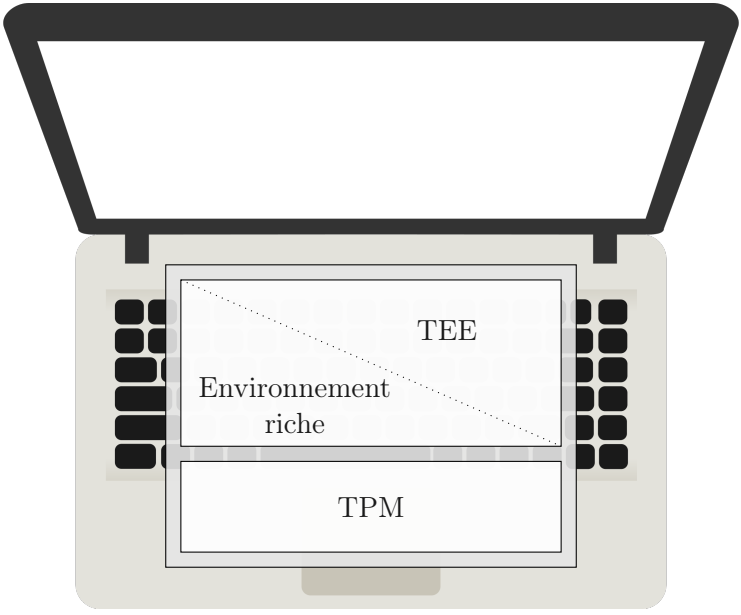
GlobalPlatform, Inc. *TEE Protection Profile*, 2020.

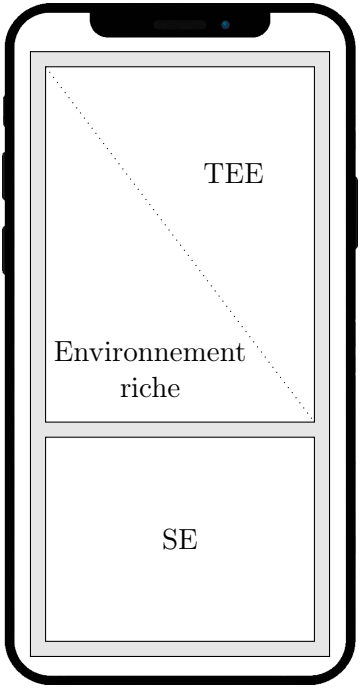
Secure Elements (SE)

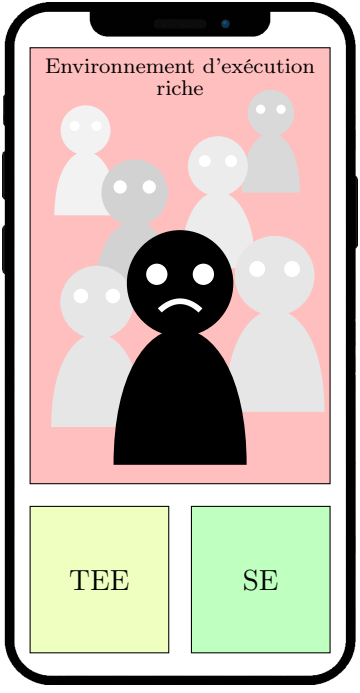
Secure Elements (SE)

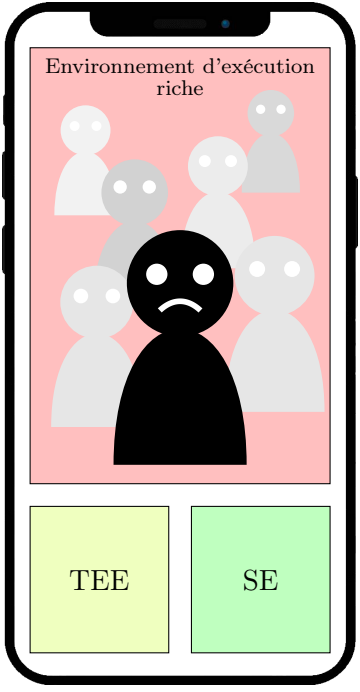

TEE
Environnement
riche
SE
HSM
TPM

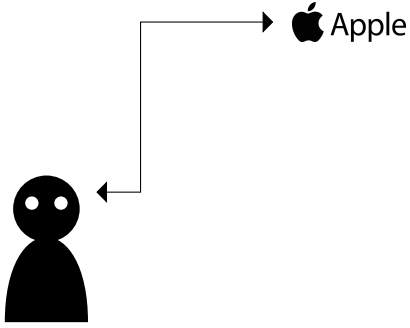

TEE
Environnement
riche
HSM
TPM

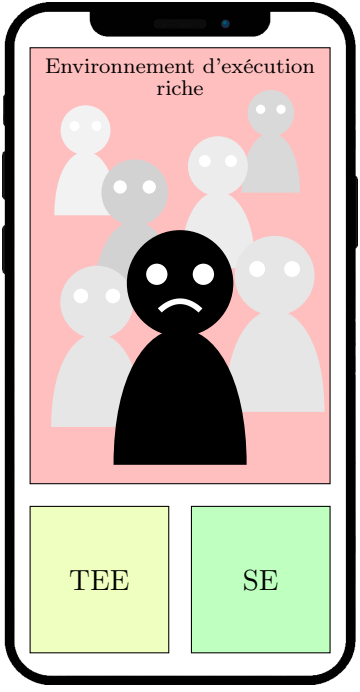

TEE
Environnement
riche
TPM

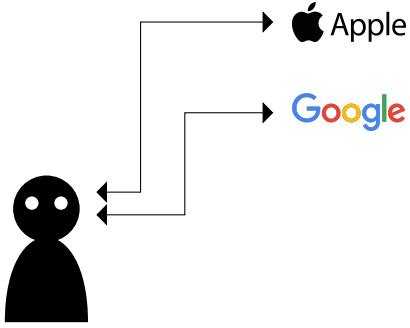

TEE
Environnement riche
SE

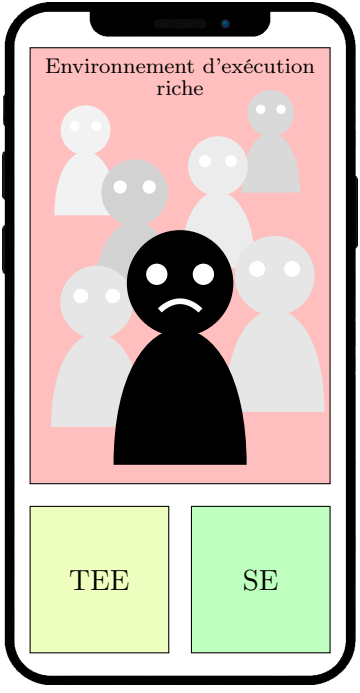

Environnement d'exécution riche
TEE
SE

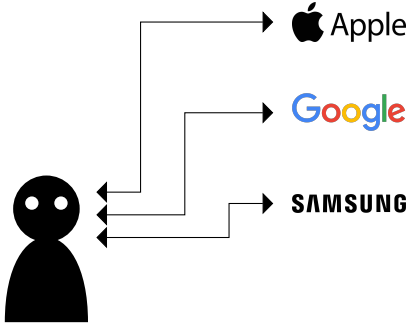

Environnement d'exécution riche
TEE
SE

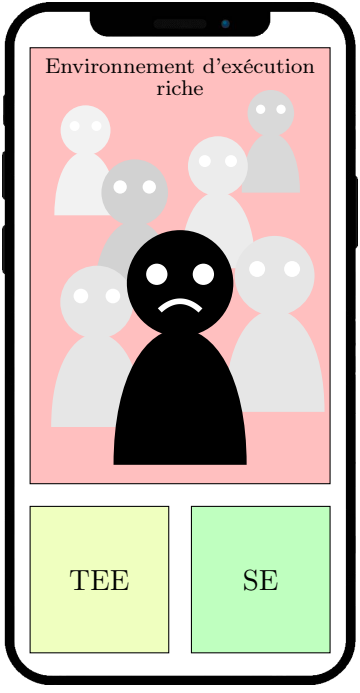

Apple

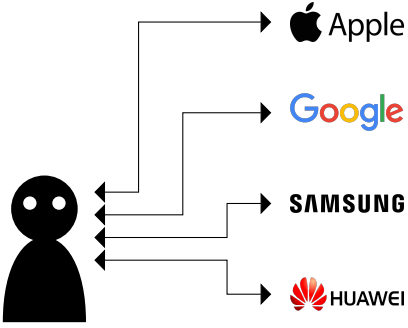

Environnement d'exécution riche
TEE
SE

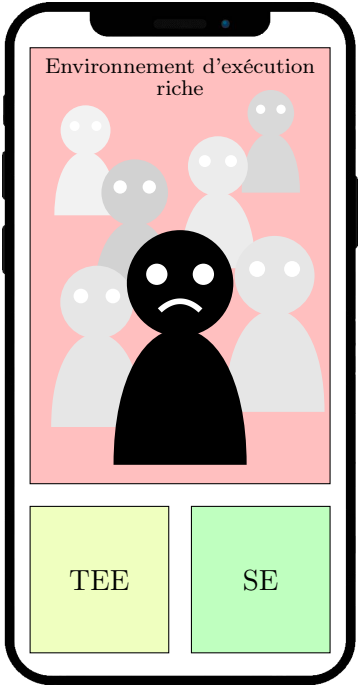

Apple
Google

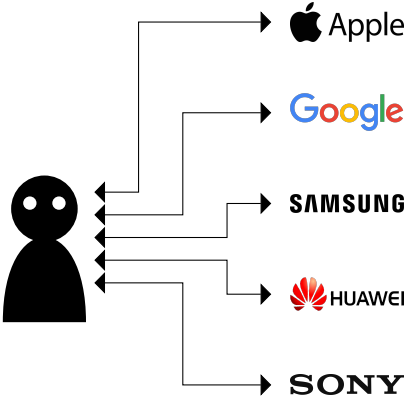

Environnement d'exécution riche
TEE
SE

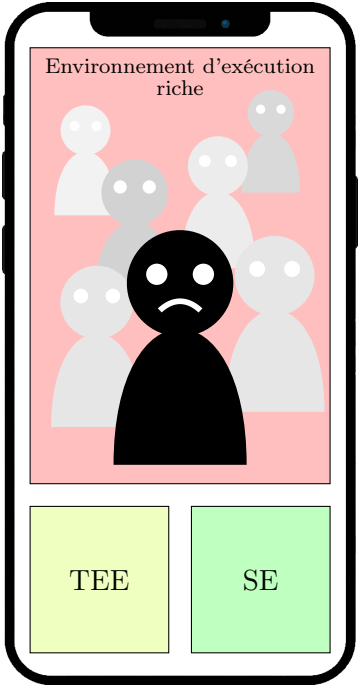

Apple
Google
SAMSUNG

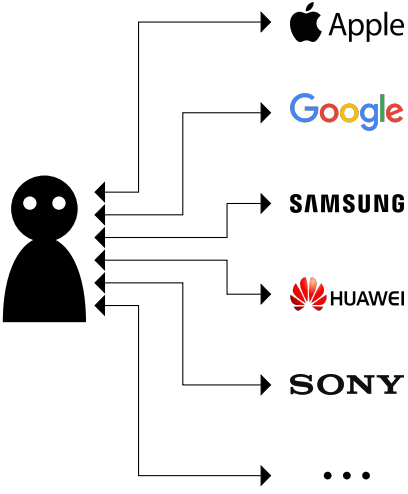

Environnement d'exécution riche
TEE
SE


Apple
Google
SAMSUNG
HUAWEI

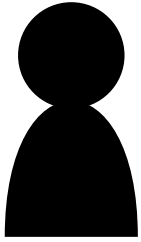

Environnement d'exécution riche
TEE
SE

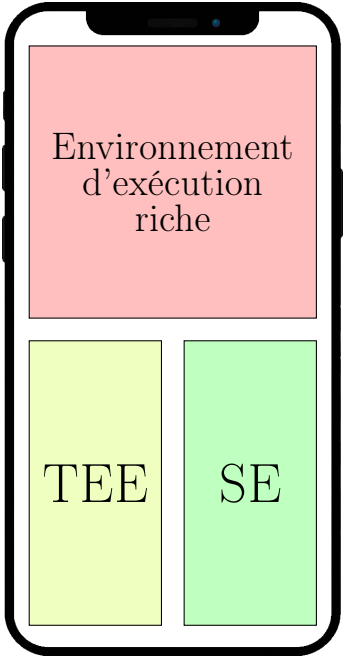

Apple
Google
SAMSUNG
HUAWEI
SONY


Environnement d'exécution riche
TEE
SE

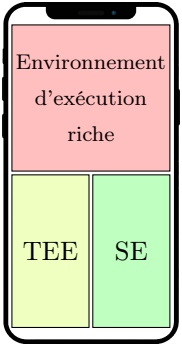

Apple
Google
SAMSUNG
HUAWEI
SONY
• • •

Utilisateur et propriétaire de la plateforme

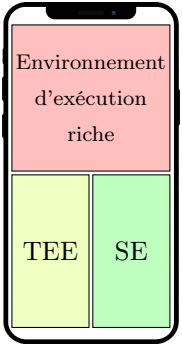




Utilisateur et propriétaire de la plateforme



Utilisateur et propriétaire de la plateforme

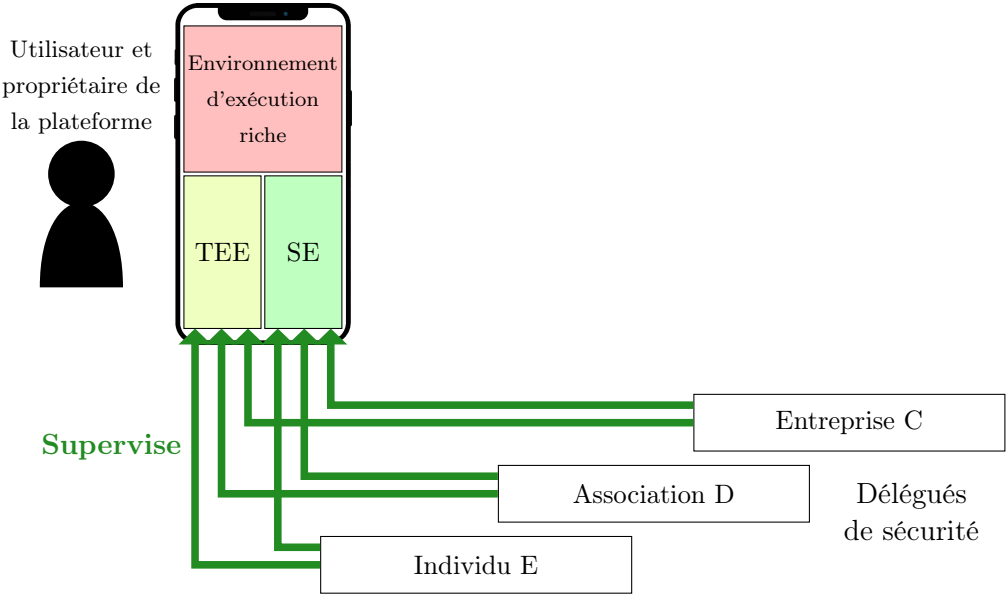


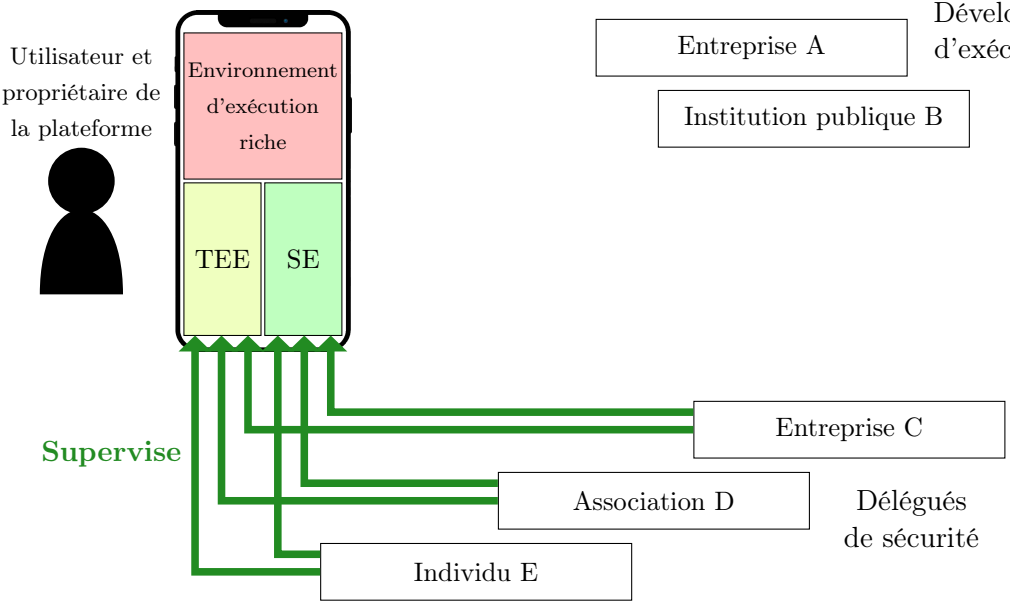
Entreprise C

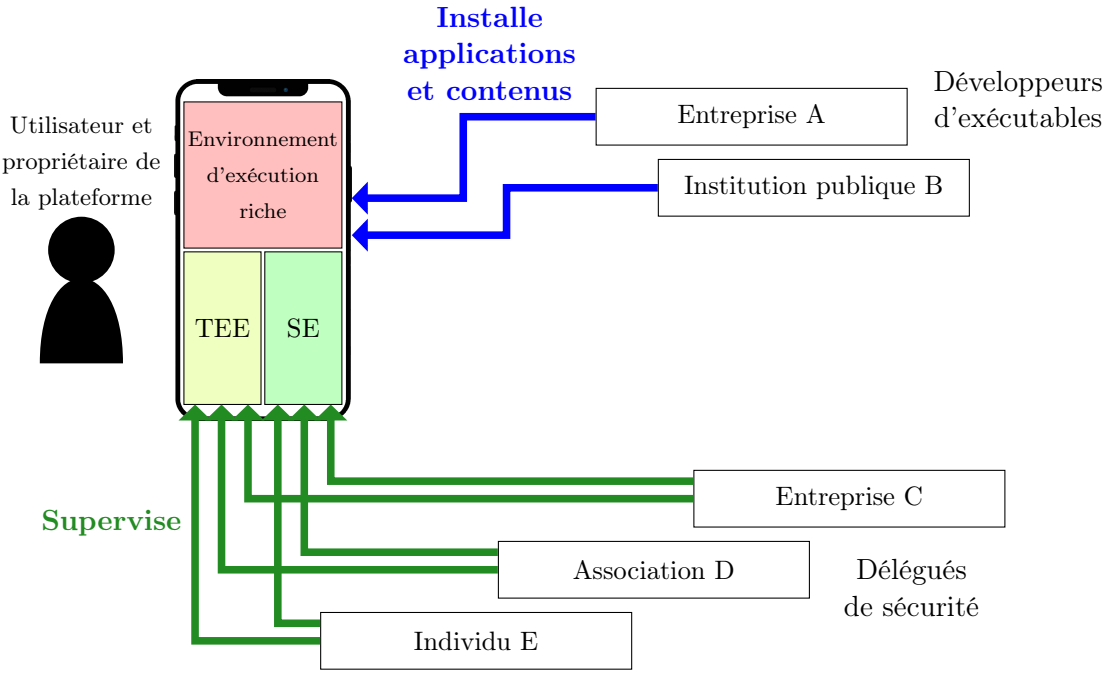
Association D

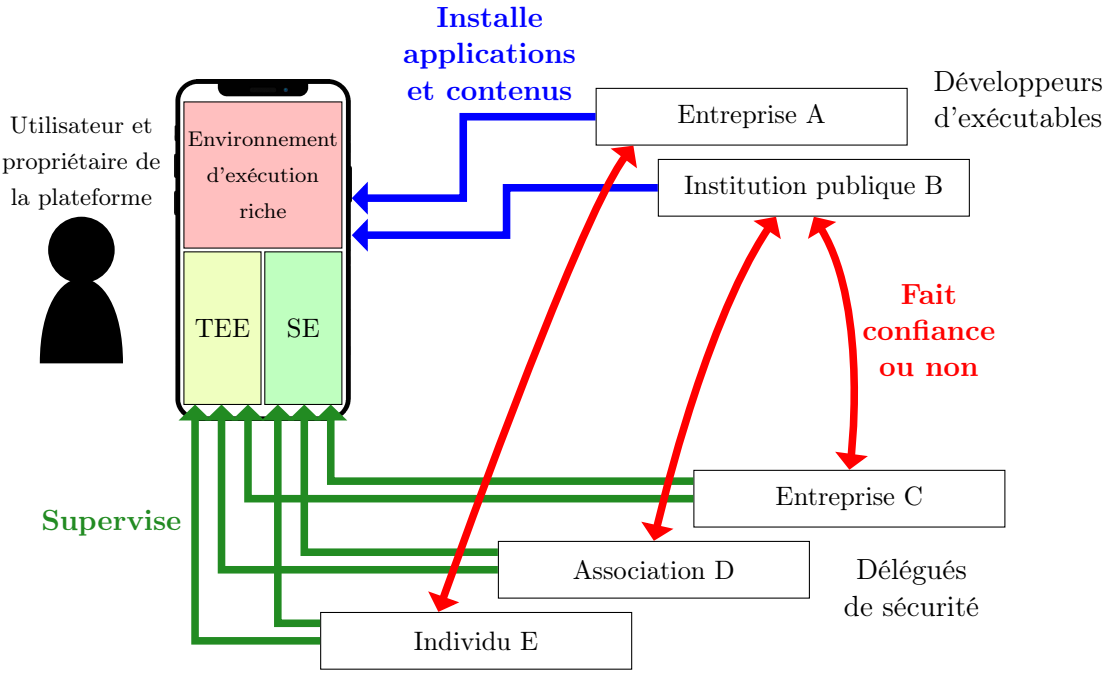
Individu E

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
Supervise
Développeurs d'exécutables
Entreprise A
Institution publique B
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

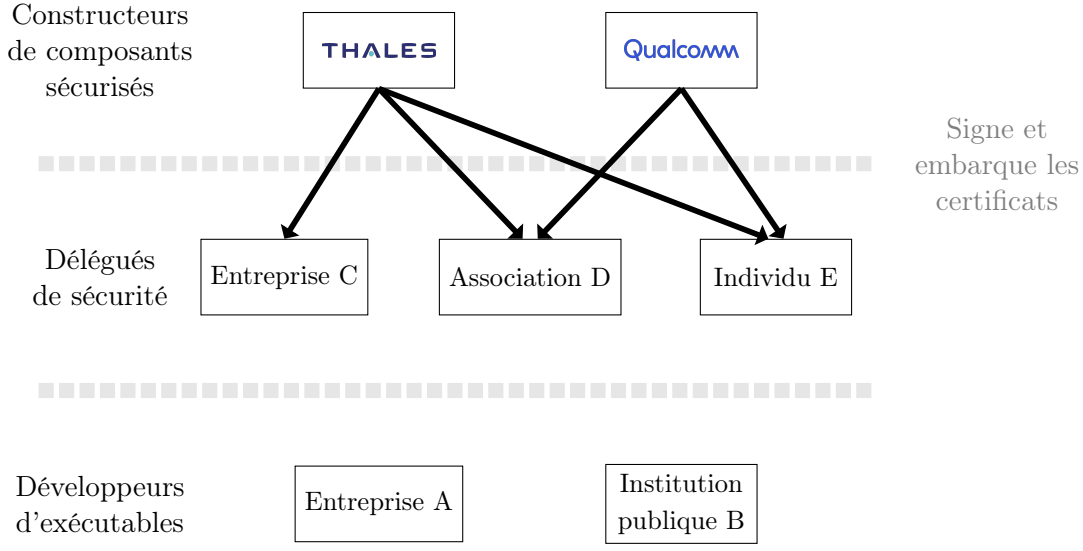
Association D

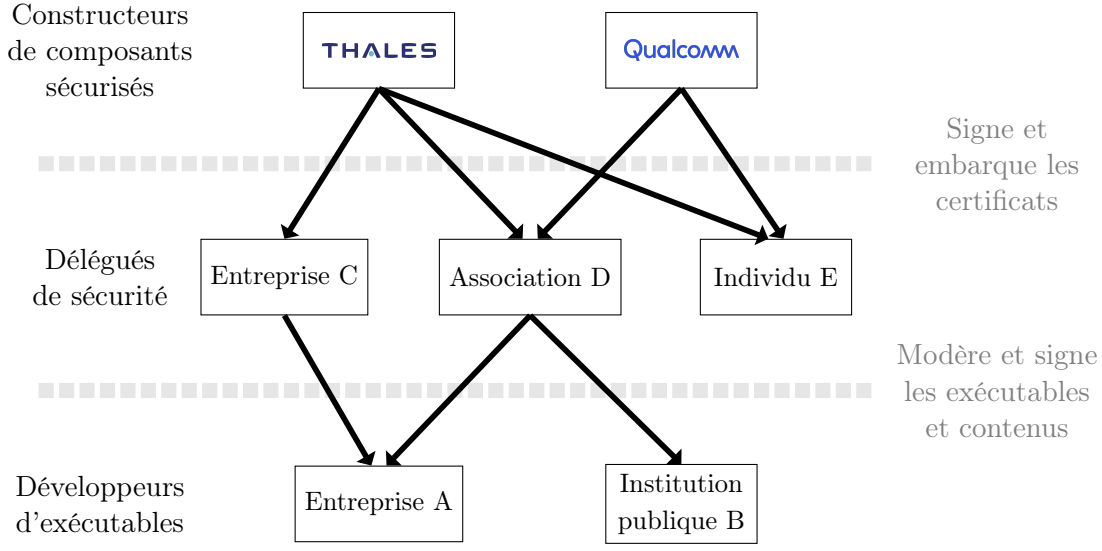
Individu E

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

GSMA™

Merci pour votre attention !