

Des environnements sécurisés indépendants rarement libres
dans vos systèmes

Vincent Giraud

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)



Secure Elements (SE)



Secure Elements (SE)



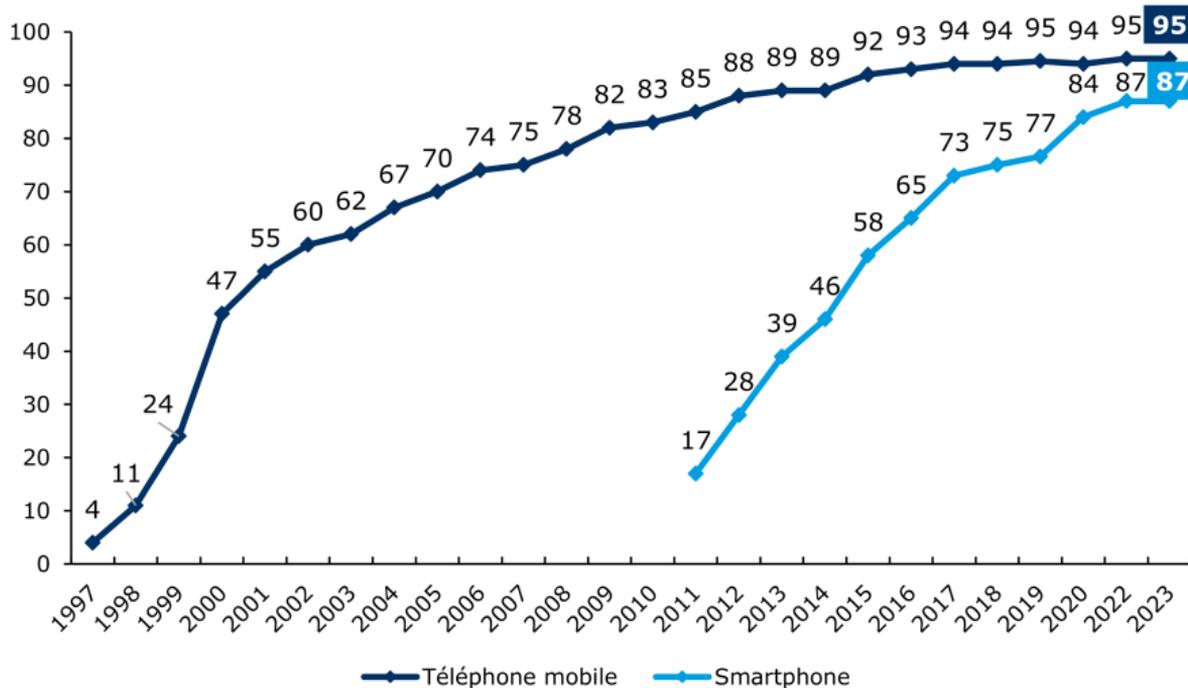


Trusted Platform Modules (TPM)



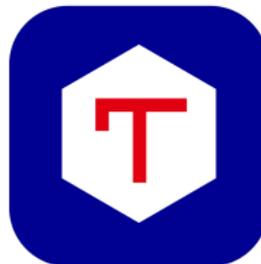
Taux d'équipement en téléphone mobile et smartphone

- Champ : ensemble de la population de 12 ans et plus, en % -



CRÉDOC, *Baromètre du numérique*, 2023.

- Communications sécurisées



- Communications sécurisées
- Stockage sécurisé

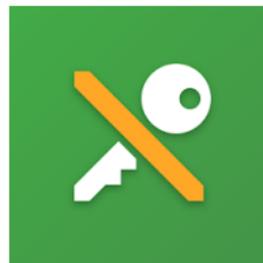
- Communications sécurisées
- Stockage sécurisé
- Biométrie

- Communications sécurisées
- Stockage sécurisé
- Biométrie
- Authentification



- Communications sécurisées
- Stockage sécurisé
- Biométrie
- Authentification

WebAuthn



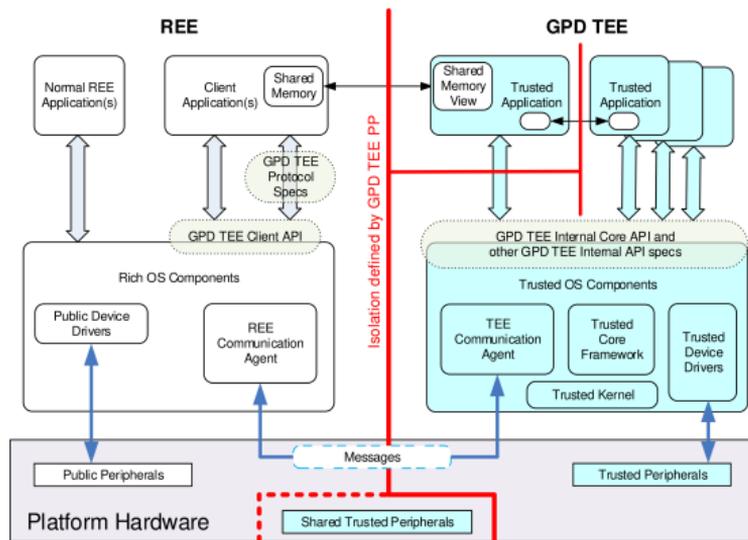
- Communications sécurisées
- Stockage sécurisé
- Biométrie
- Authentification
- Transport



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

The logo for Apple Pay, featuring a black silhouette of an apple with a bite taken out of it, followed by the word "Pay" in a bold, black, sans-serif font.The logo for Google Pay, featuring the multi-colored "G" logo of Google, followed by the word "Pay" in a grey, sans-serif font.The logo for Samsung Pay, featuring the word "SAMSUNG" in a bold, black, sans-serif font, with the word "Pay" in a smaller, black, sans-serif font below it.

Trusted Execution Environments (TEE)



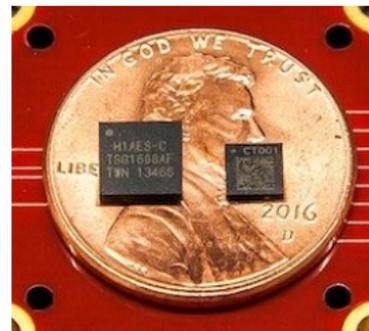
Key		TEE Isolation Boundary (Defined by TEE PP)	
↕	Shared, or synchronized, Memory Image	—	Fixed Isolation boundary
↕↔	Low level message routing	⋯	Transferable Isolation – Some peripherals may be shared. Such sharing must be under the control of other hardware under permanent control of the TEE.
↕↔	Application interfaces		

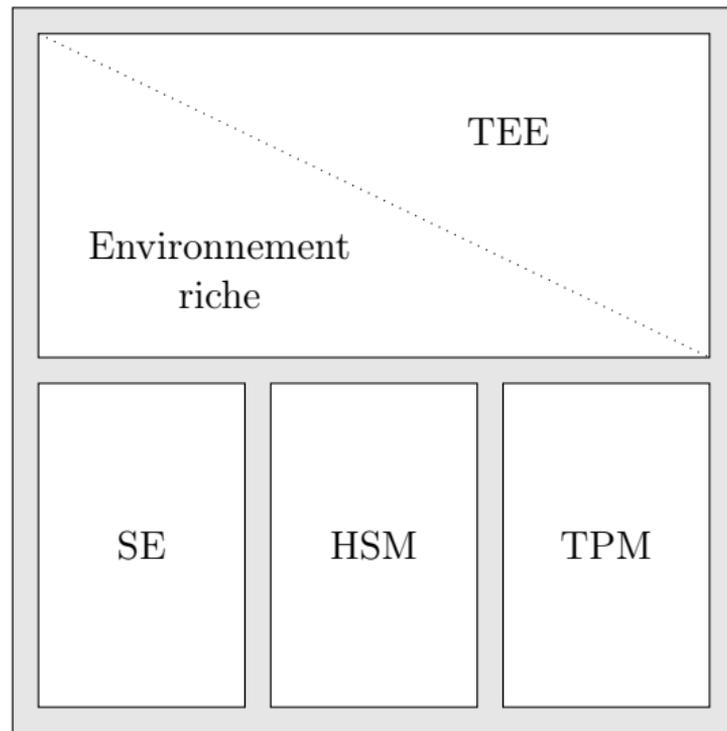
GlobalPlatform, Inc. *TEE Protection Profile*, 2020.

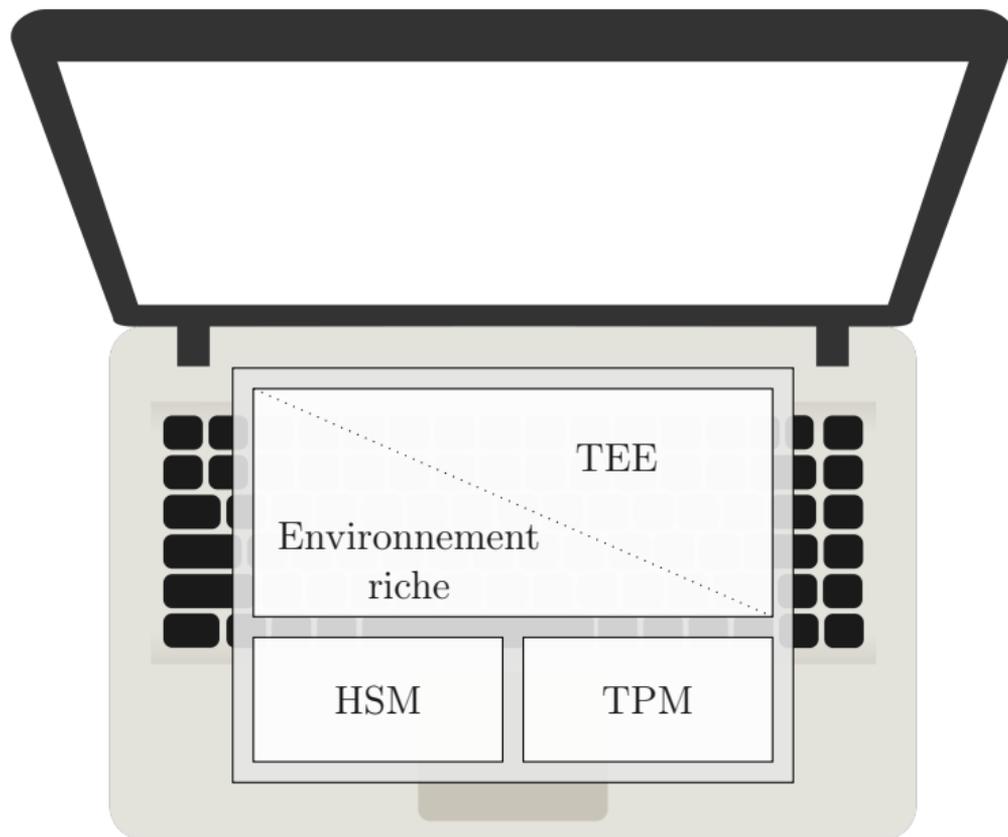
Secure Elements (SE)

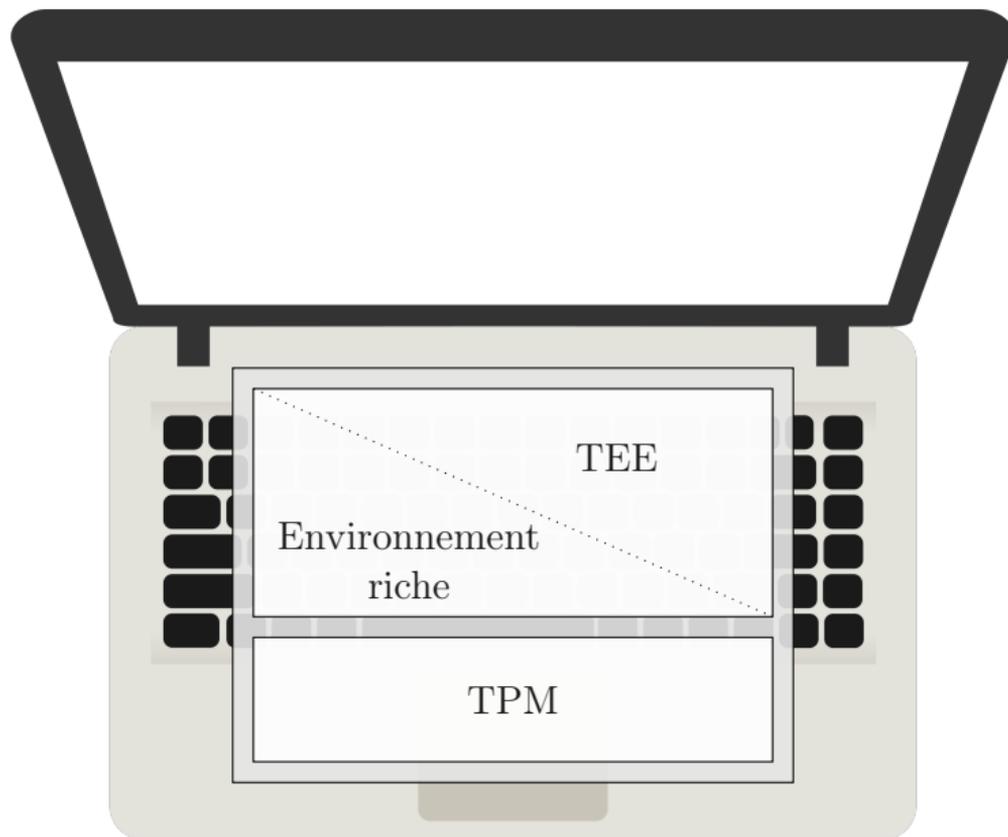


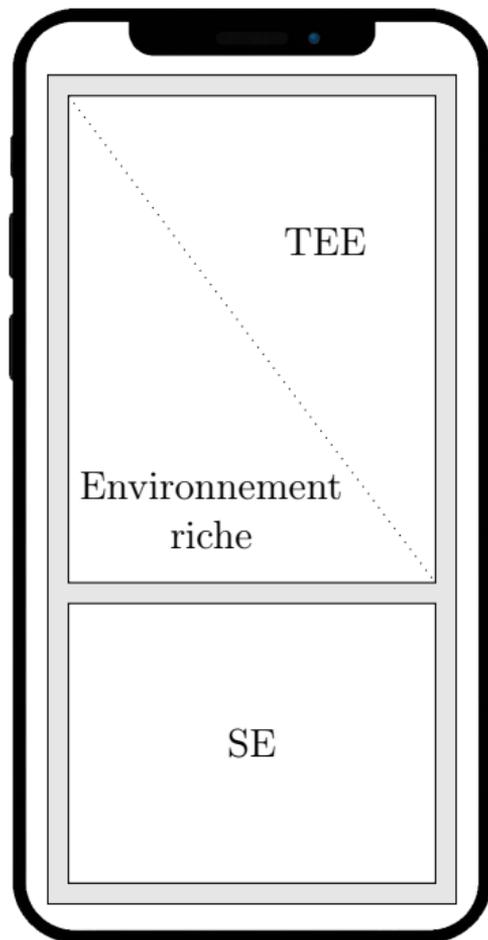
Secure Elements (SE)

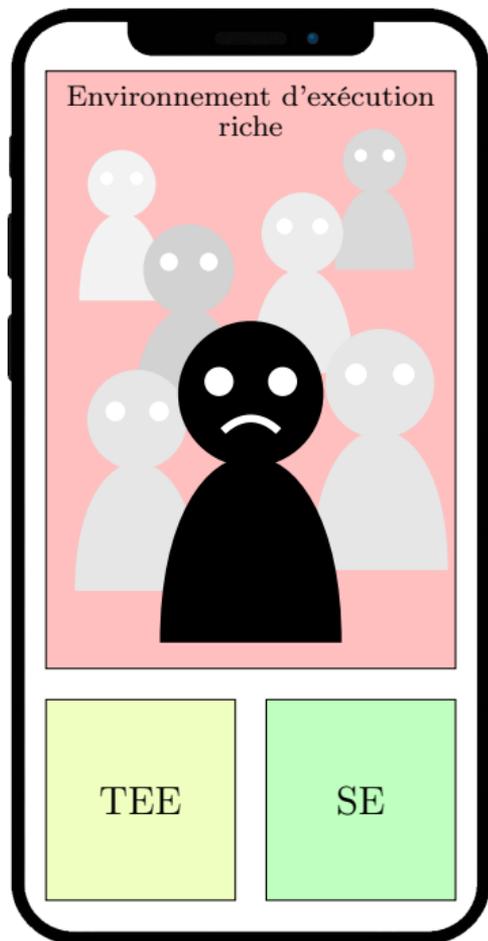


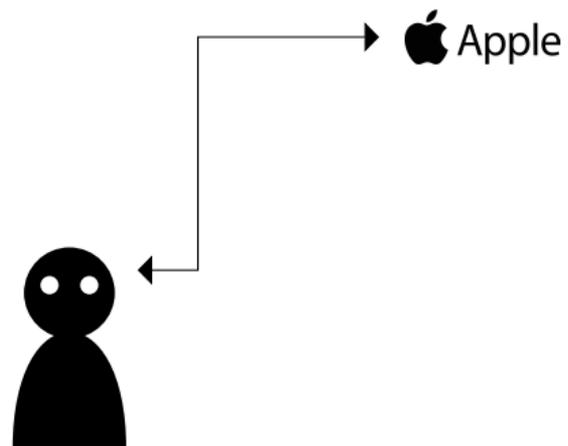
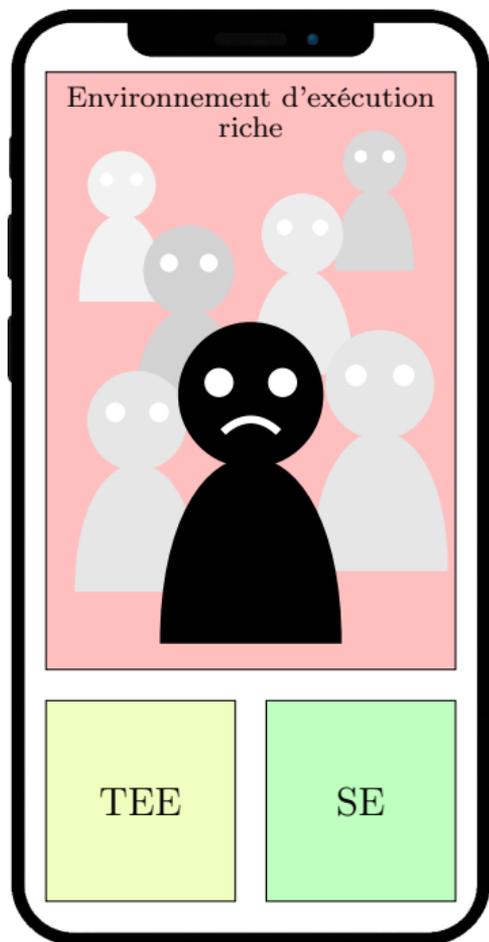


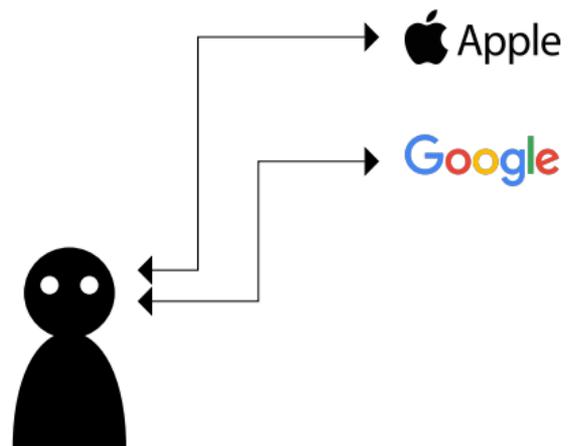
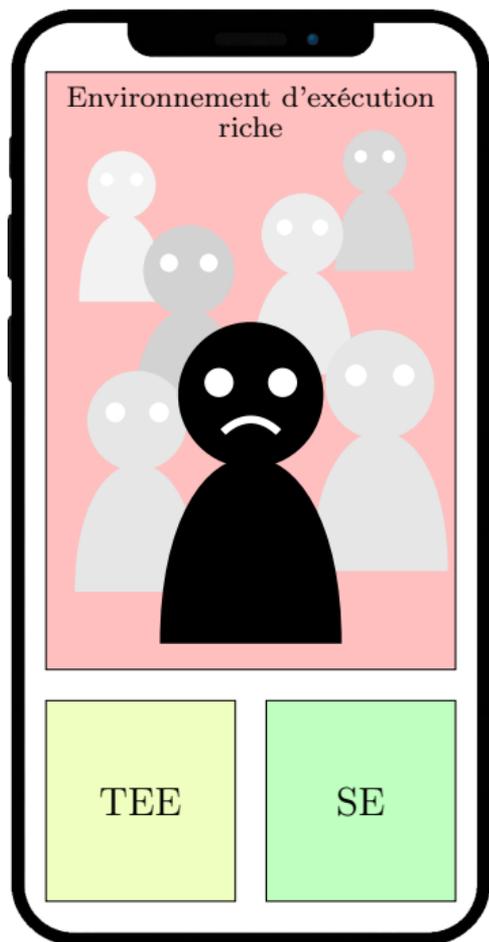


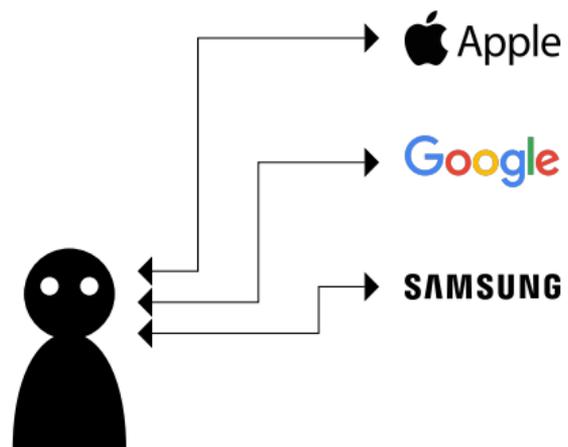
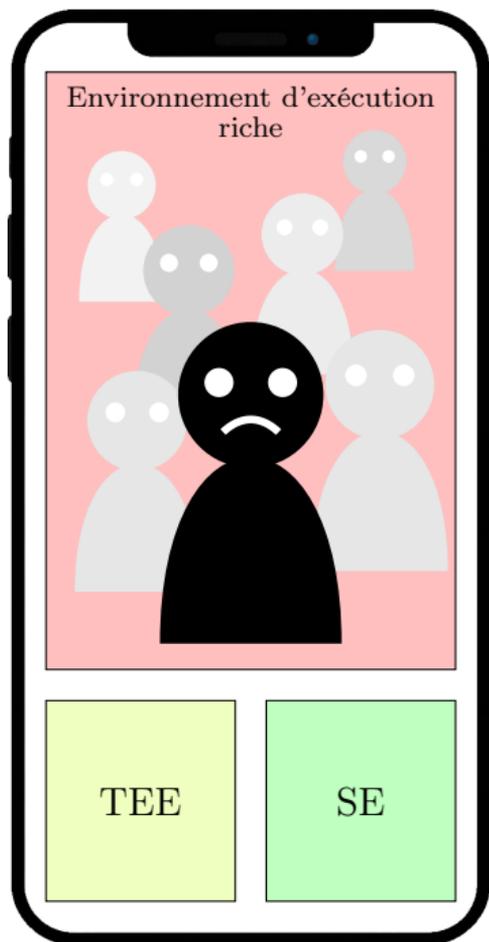


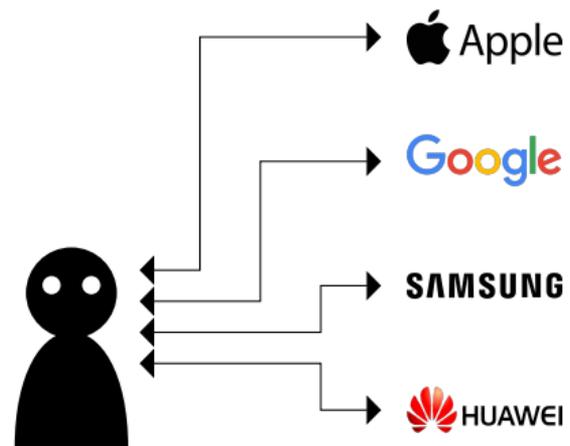
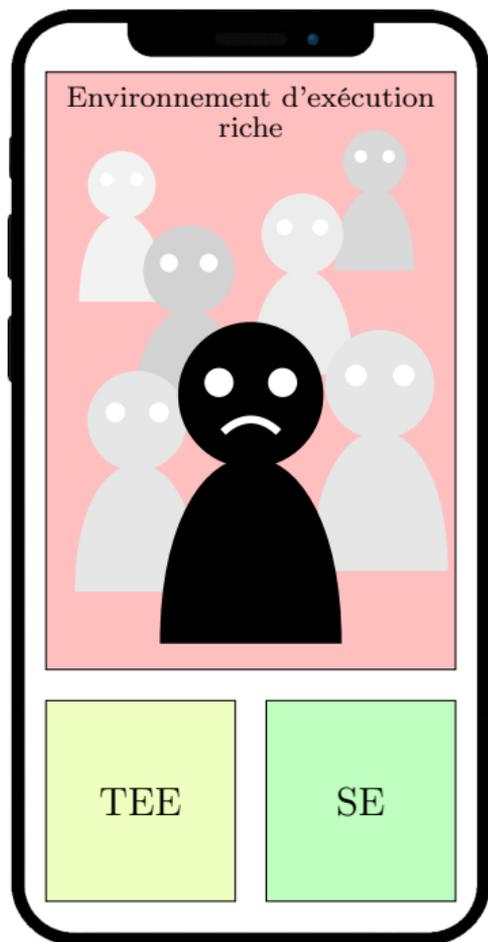


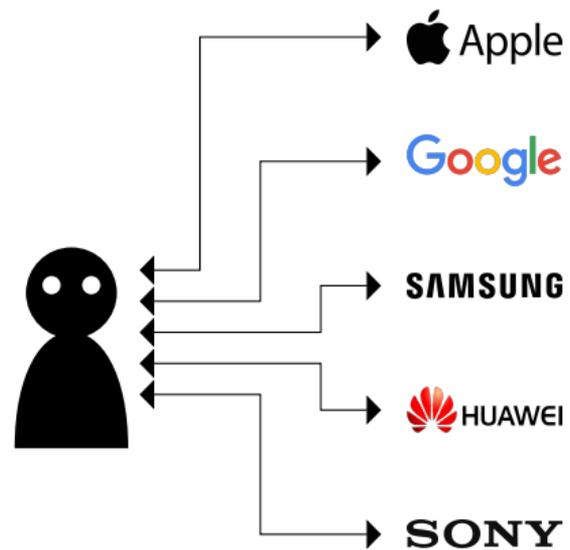
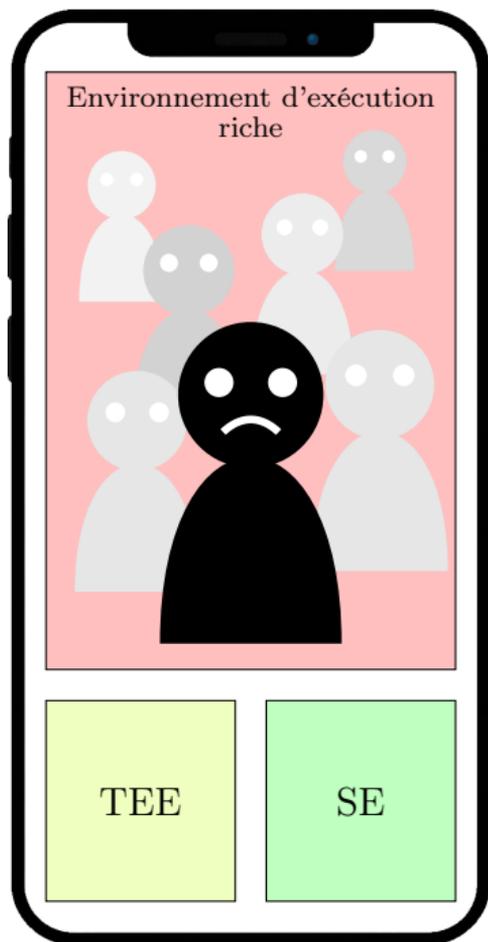


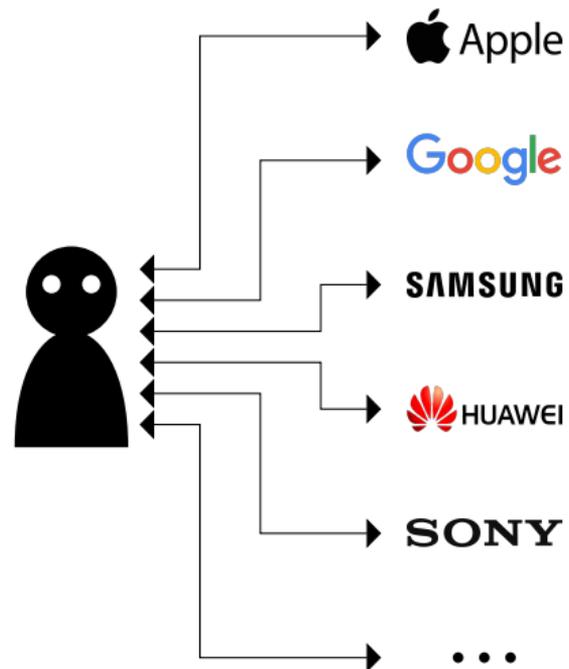
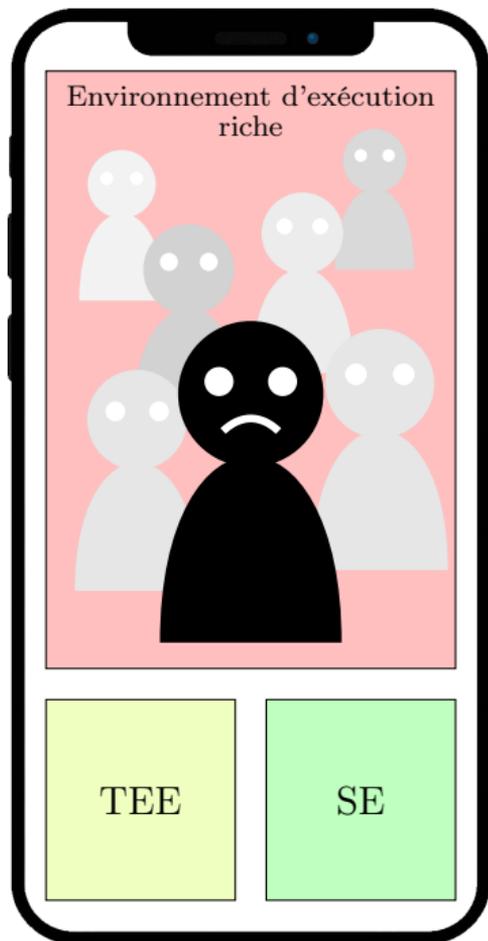




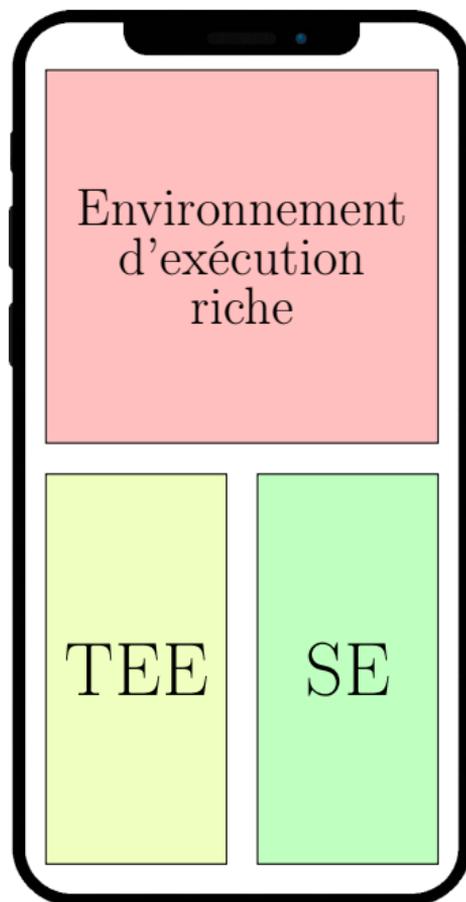
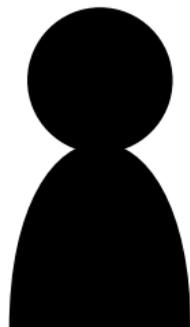




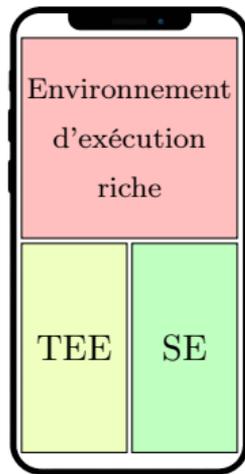




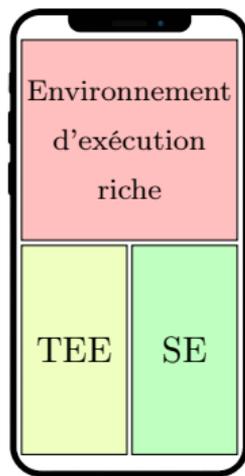
Utilisateur et
propriétaire de
la plateforme



Utilisateur et
propriétaire de
la plateforme



Utilisateur et
propriétaire de
la plateforme

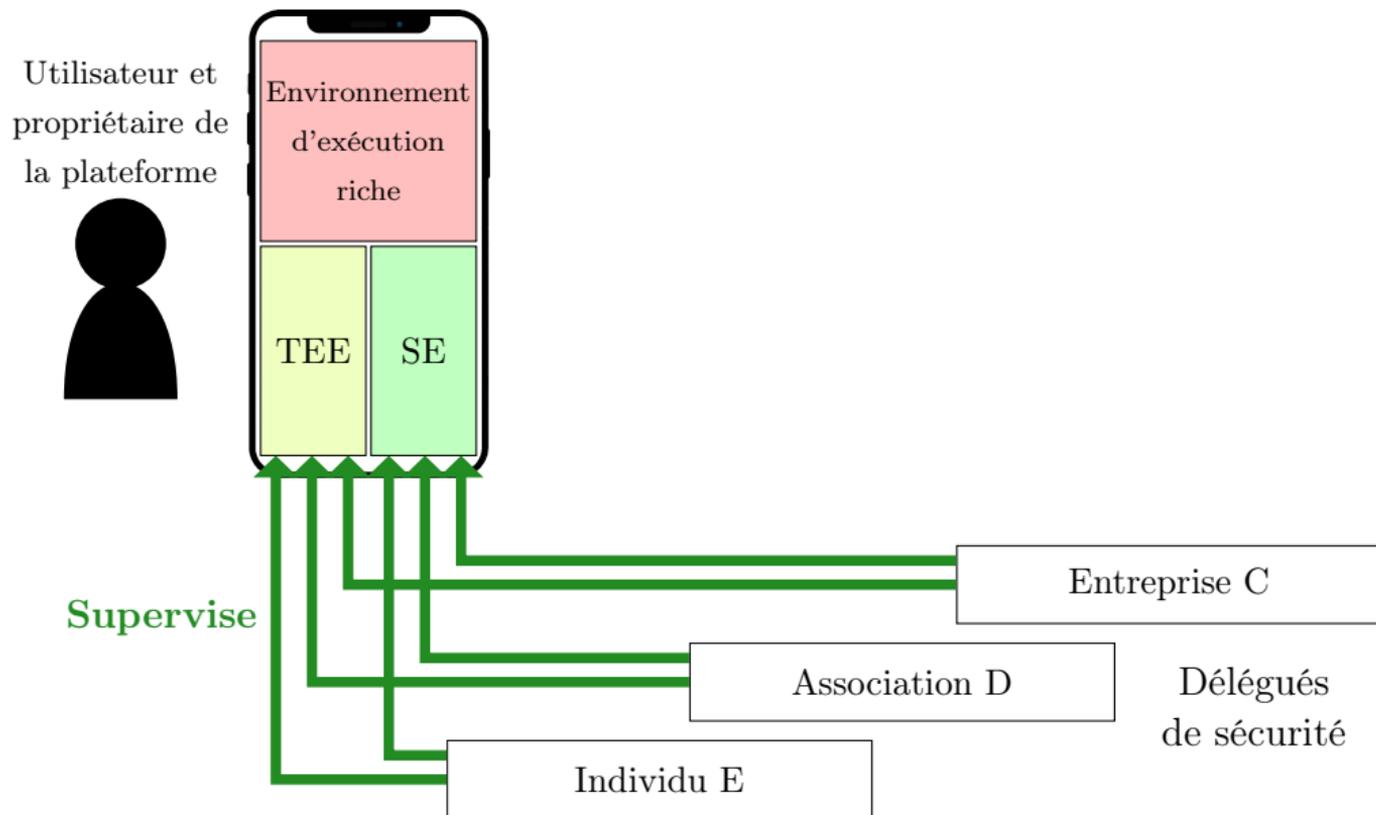


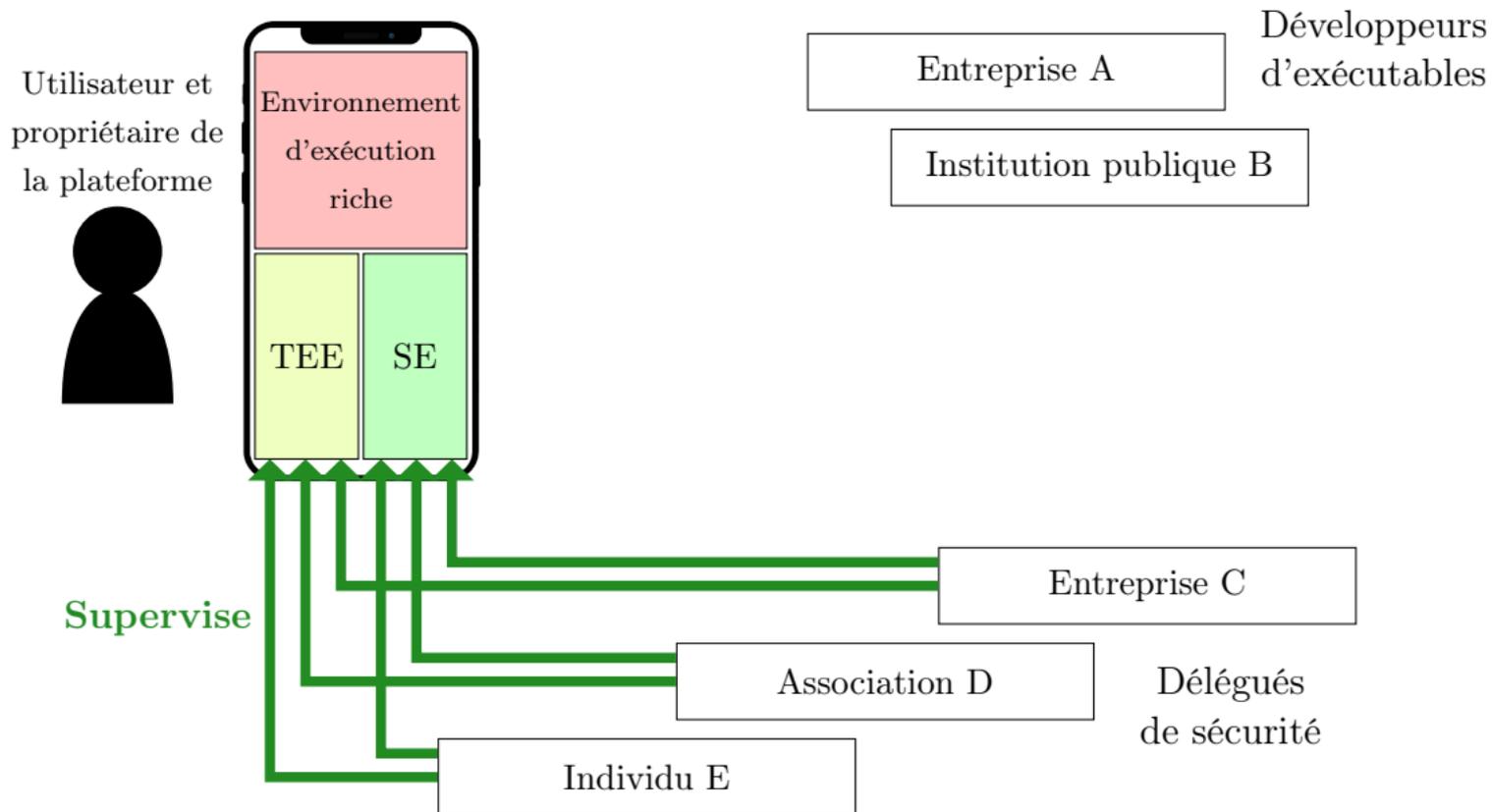
Entreprise C

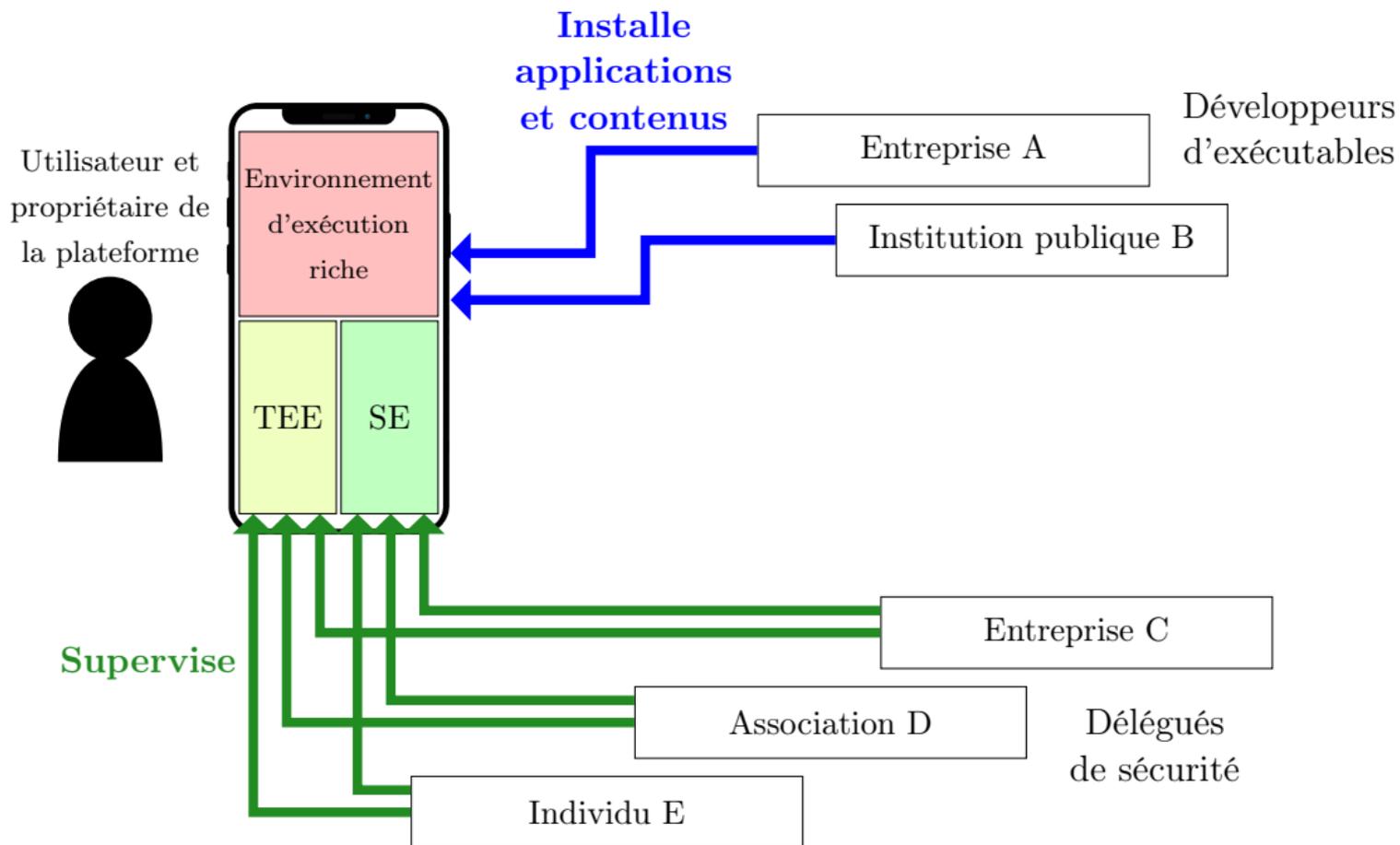
Association D

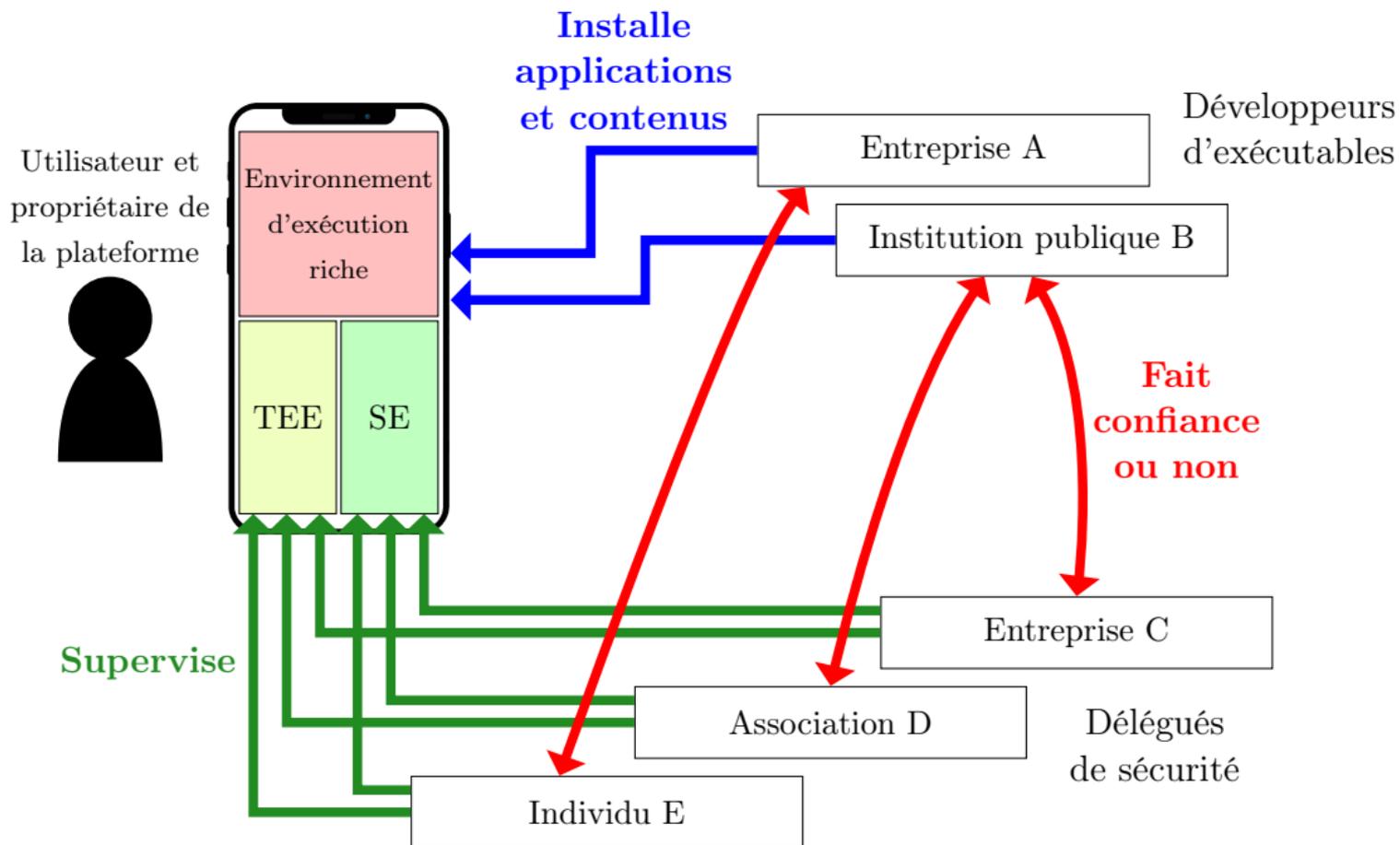
Délégués
de sécurité

Individu E









Constructeurs
de composants
sécurisés

THALES

Qualcomm



Délégués
de sécurité

Entreprise C

Association D

Individu E



Développeurs
d'exécutables

Entreprise A

Institution
publique B

Constructeurs
de composants
sécurisés

THALES

Qualcomm



Délégués
de sécurité

Entreprise C

Association D

Individu E

Signe et
embarque les
certificats



Développeurs
d'exécutables

Entreprise A

Institution
publique B

Constructeurs
de composants
sécurisés

THALES

Qualcomm

Délégués
de sécurité

Entreprise C

Association D

Individu E

Signe et
embarque les
certificats

Développeurs
d'exécutables

Entreprise A

Institution
publique B

Modère et signe
les exécutables
et contenus

Constructeurs

de cor
séc



GSMA™

ne et
rque les
ificats

Dé
de s

e et signe
cutables
ntenus

Déve
d'exécutables

publique D

Merci pour votre attention !