À la croisée de l'informatique confidentielle et des technologies Trustless !

Étienne Bossé - 13/06/2023

Qui sommes-nous ?

secretarium | klave

Partenaires & adoptants

THALES intel IQ CAPITAL Open Trusted Cloud™

Introduction: BigData, Confidentialité et Cybersécurité

2016
90% données générées les 2 années précédentes, 1% analysé.
McKinsey, 2016

2022
84% des entreprises accordent le plus d'importance à la gestion de la confidentialité lors de l'achat de logiciel.
Gartner, 2022

2023
75% de la population mondiale sera couverte par des régulations sur les données privées.
Gartner, 2023

2025
60% des organisations vont traiter la cybersécurité comme risque N°1.
Gartner, 2023


Confiance


Honnêteté


Confidentialité


Sécurité

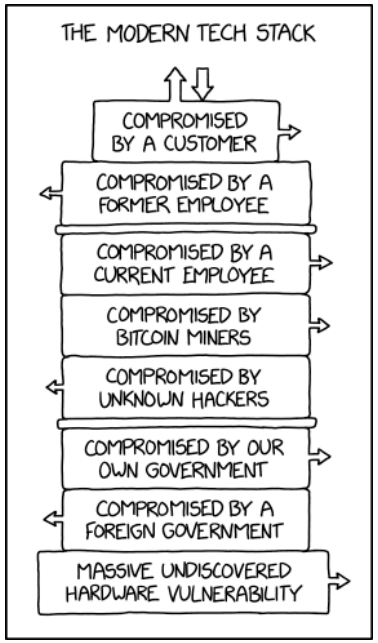
La confiance c'est quoi ?

"C'est un sentiment d'assurance..."

Confiance dans les intermédiaires

- Basé sur la réputation
- Coûteux
- Frein à l'innovation
- Souvent toujours très risqué
- Sujet à l'erreur

Confiance dans les systèmes d'informations



From https://xkcd.com/2166/

Objectif: Limiter la confiance au maximum

Principes de conception de Klave

Honnêteté et vérifiabilité

- Attestation
- Preuve Cryptographique

Limiter la confiance

- Approche Zéro confiance
- Limiter la confiance dans les tierces parties

Confidentialité et Sécurité

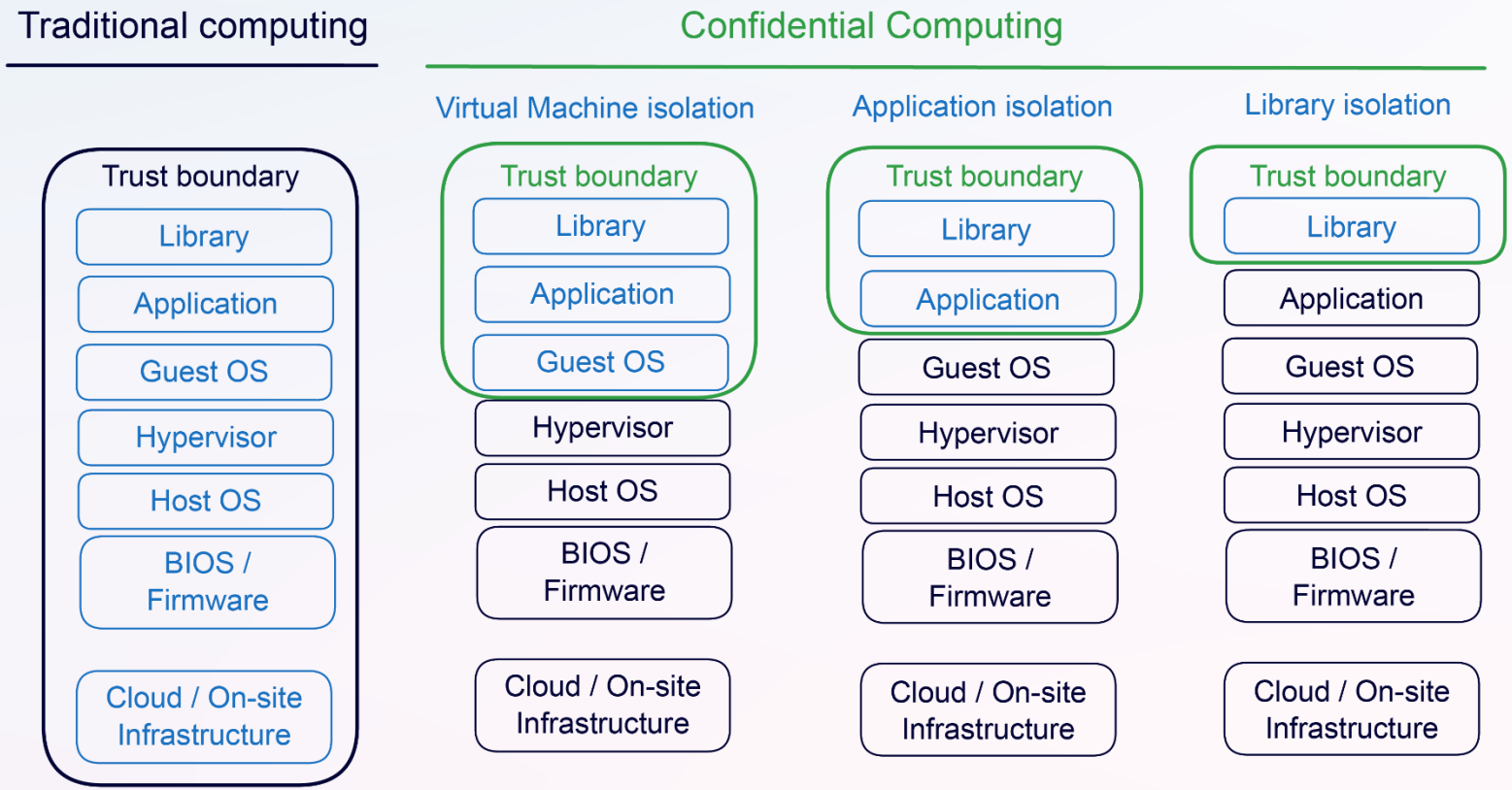
- Intégrité calculatoire
- Intégrité des données
- Cryptographie avancée

Développeurs au centre

- Workflow intégration
- Langages de haut niveau
- Cycle de vie de l'Application

L'informatique confidentielle

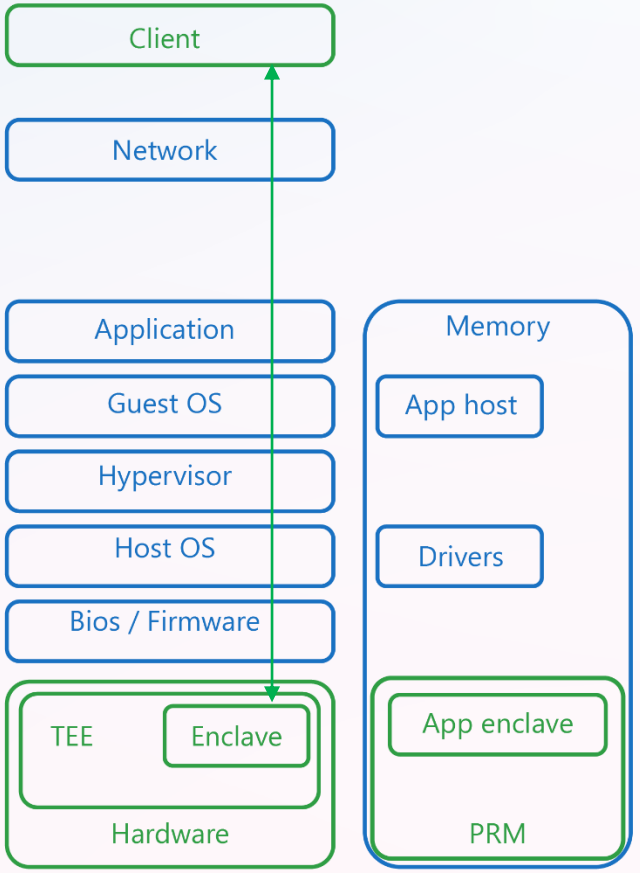
L'informatique confidentielle apporte des couches supplémentaires de sécurité pour protéger la logique business et préserver la confidentialité et l'intégrité des données pendant leur utilisation.



Environnement d’exécution de confiance & Enclave

L'informatique confidentielle est base sur l'utilisation des environnements d’exécution de confiance qui apportent les garanties suivantes:

- Intégrité des données
- Confidentialité des données
- Intégrité du code
- Confidentialité du code
- Attestable
- Programmable
- Optimisation hardware pour la cryptographie



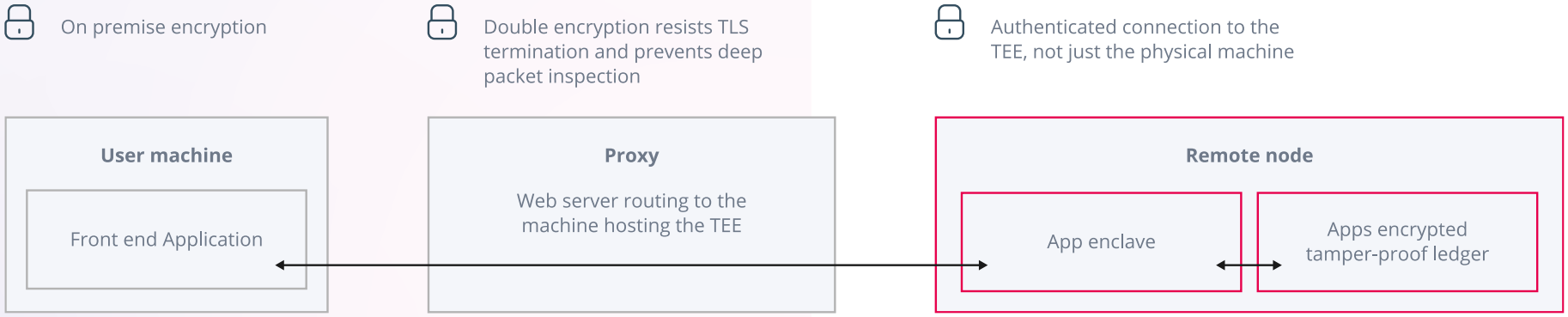
Management des enclaves: EnclOS

Enclave OS (EnclOS), est le système d'exploitation sécurisé que nous avons mis au point pour apporter toutes les fonctionnalités nécessaires aux enclaves.

- Communications
- Systèmes de fichiers
- Traçage

Modèle de sécurité:

- Manipulation de hash
- Merkle proof
- Attestation locale & distante
- Signature digitale
- SMPC
- Secret sharing



klave

Architecture distribuée et DLT

- Pour assurer une haute disponibilité et une continuité des opérations
- DLT, base de données distribuées synchronise en quasi-temps réel.
- Algorithme de consensus RAFT (state machine)
- Logchain pour garder l'intégrité
- Byzantine Fault Tolerance RAFT
- Architecture sensible aux objectifs verts

Klave c'est quoi ?

Plateforme Trustless

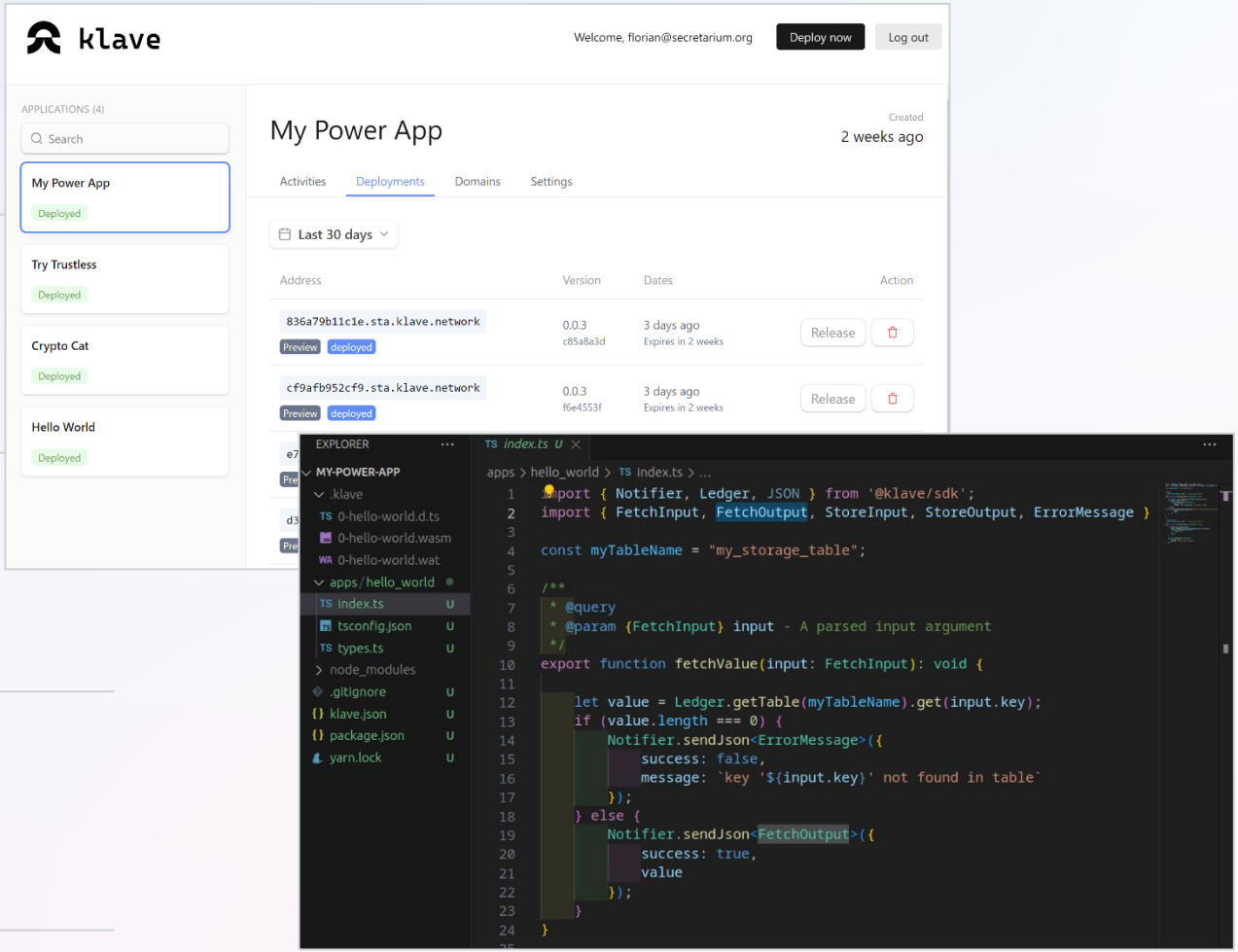
- Intégrité des données & confidentialité
- Resistance à la fraude & intégrité de calcul
- Vérifiable & Honnête

Klave App

- Turing complete
- État persistant
- Confidentialité
- Intégrité
- Isolation
- Vérifiable

Développeur au centre

- SDK simple
- Langages haut niveau
- Intégration avec l'environnement



Ramener la responsabilité dans la logique business

Register to the beta now at klave.network/beta

Thank you!