

An introduction to confidential computing

Smals Research

Agenda

General overview

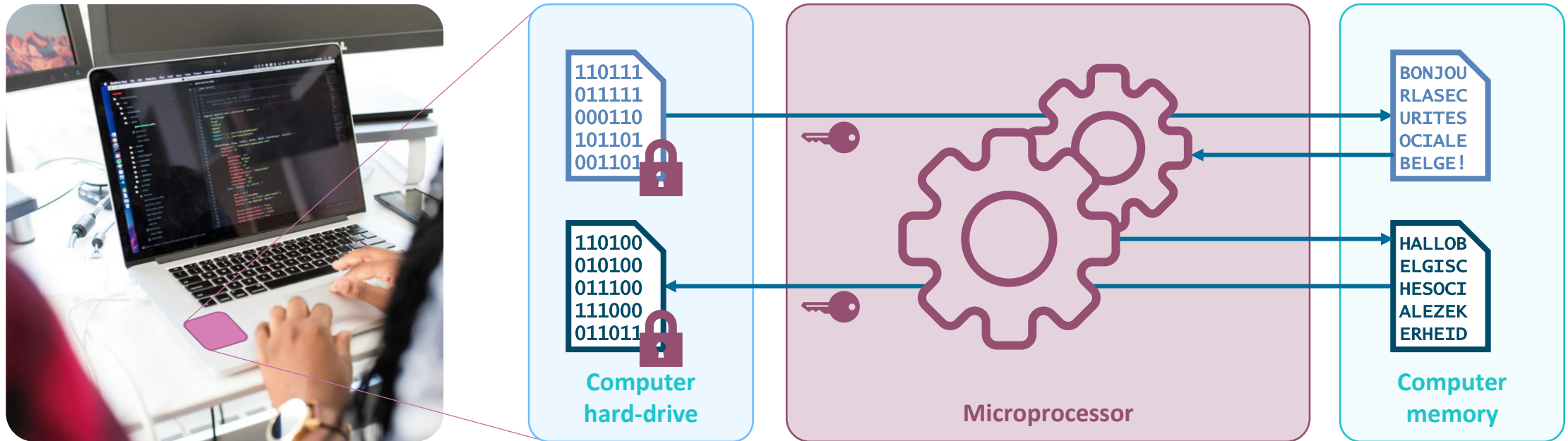
-
-
-
-
-

Market offer for TEE

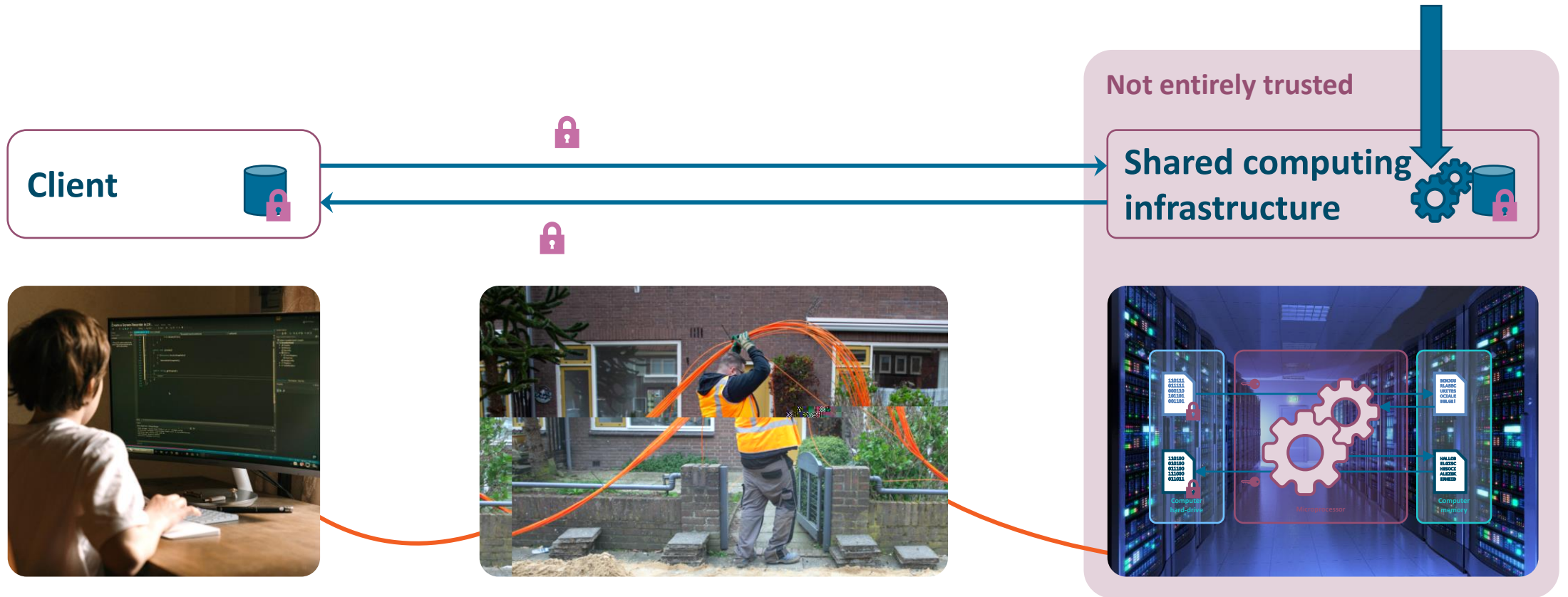
-
-

Conclusions and recommendations

Traditional computation on encrypted data

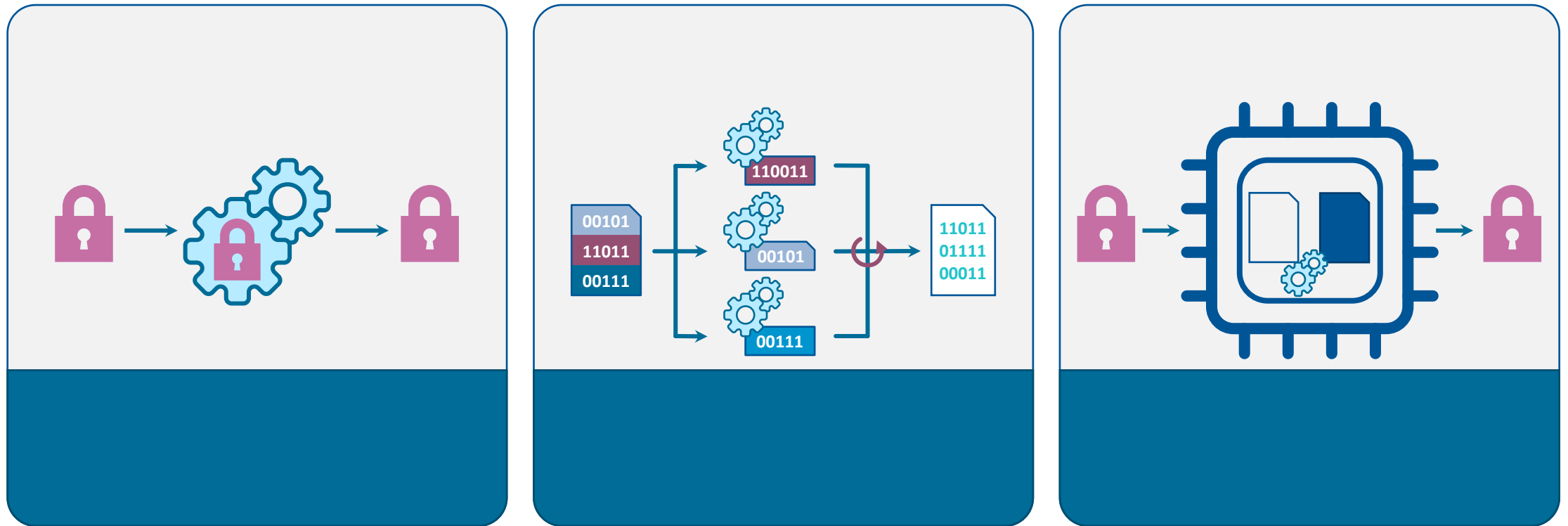


Basic remote computation



Main techniques for trusted remote computation

Aim: move the infrastructure provider outside of the trust boundary



Homomorphic encryption (HE)

Homomorphic encryption: schematic overview

Client



Shared computing infrastructure



(f)

f

⋮



Is

Advantages and limits of homomorphic encryption

Pros

-

-

-

-

Cons

-

-

-

- $[[m_1]] \ominus [[m_2]]$

- $[[m_1]] \oplus [[m_2]]$

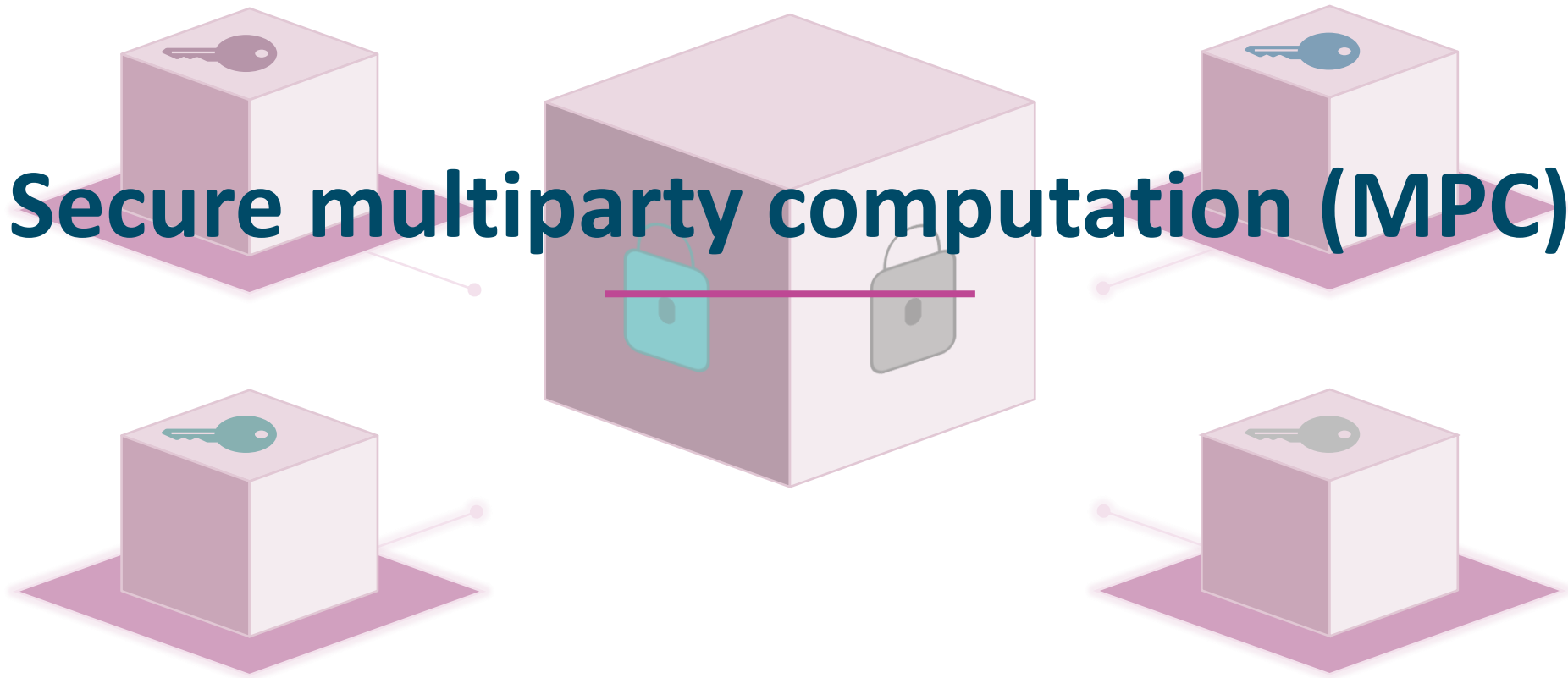
-

-

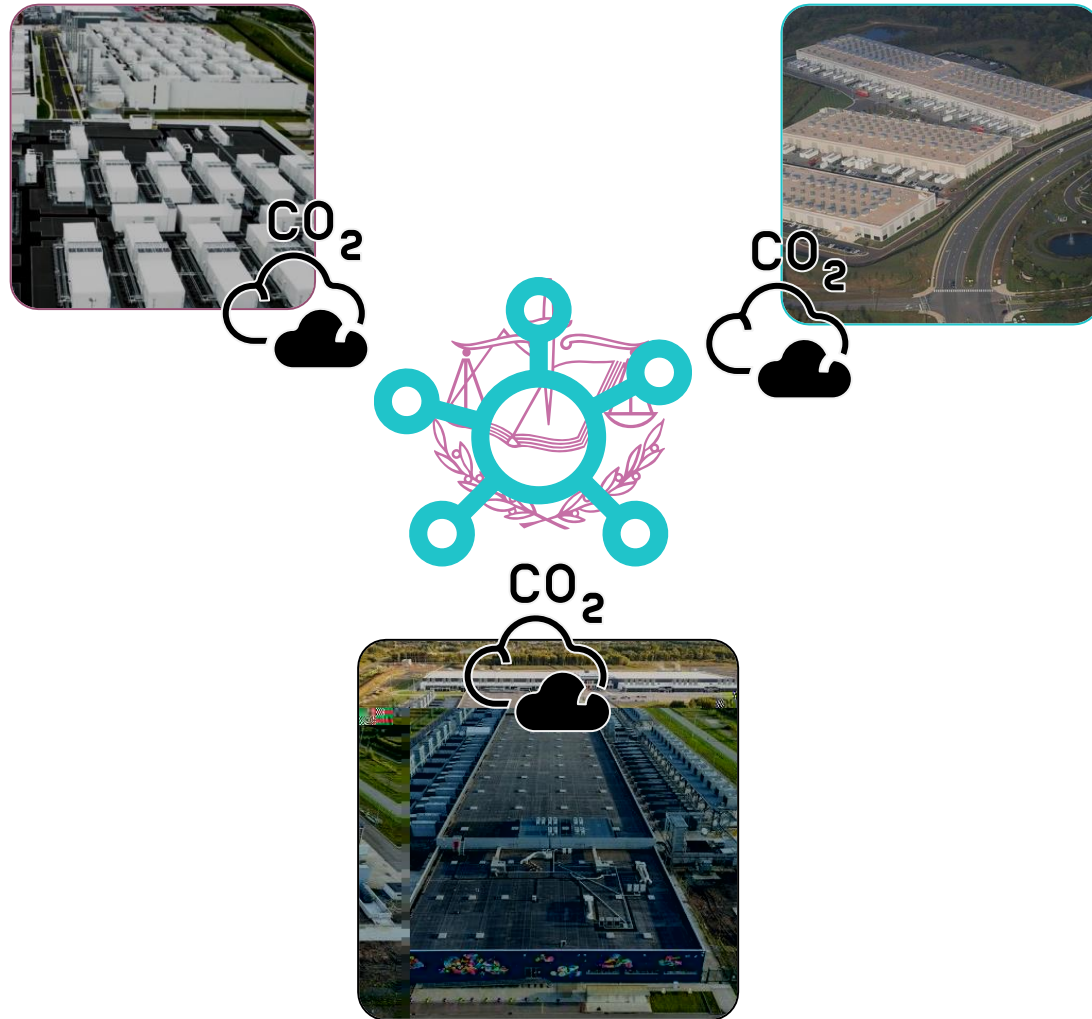
-

-

Secure multiparty computation (MPC)



MPC problem example



MPC problem and α solution

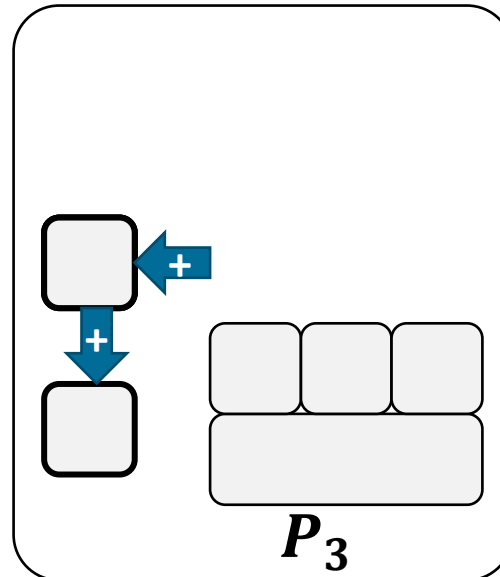
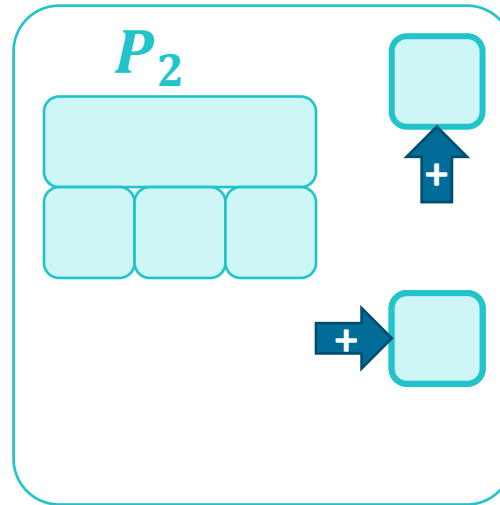
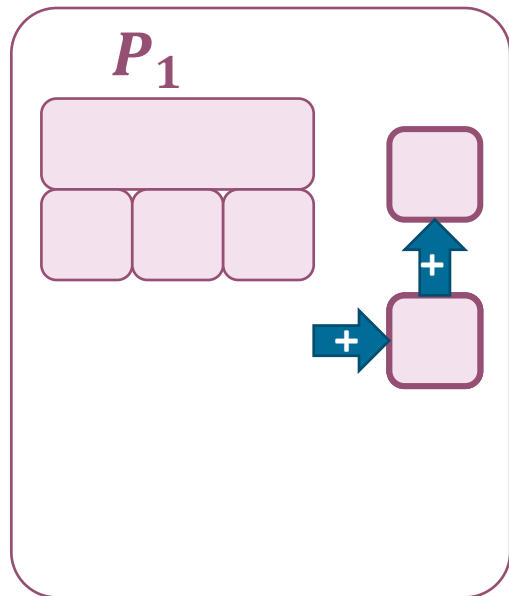
• Problem n P_1, \dots, P_n x_i f

- $z = f(x_1, \dots, x_n)$
- x_1, \dots, x_n

• MPC solution example

- f + \times
-
-
-

MPC in action: simple addition example

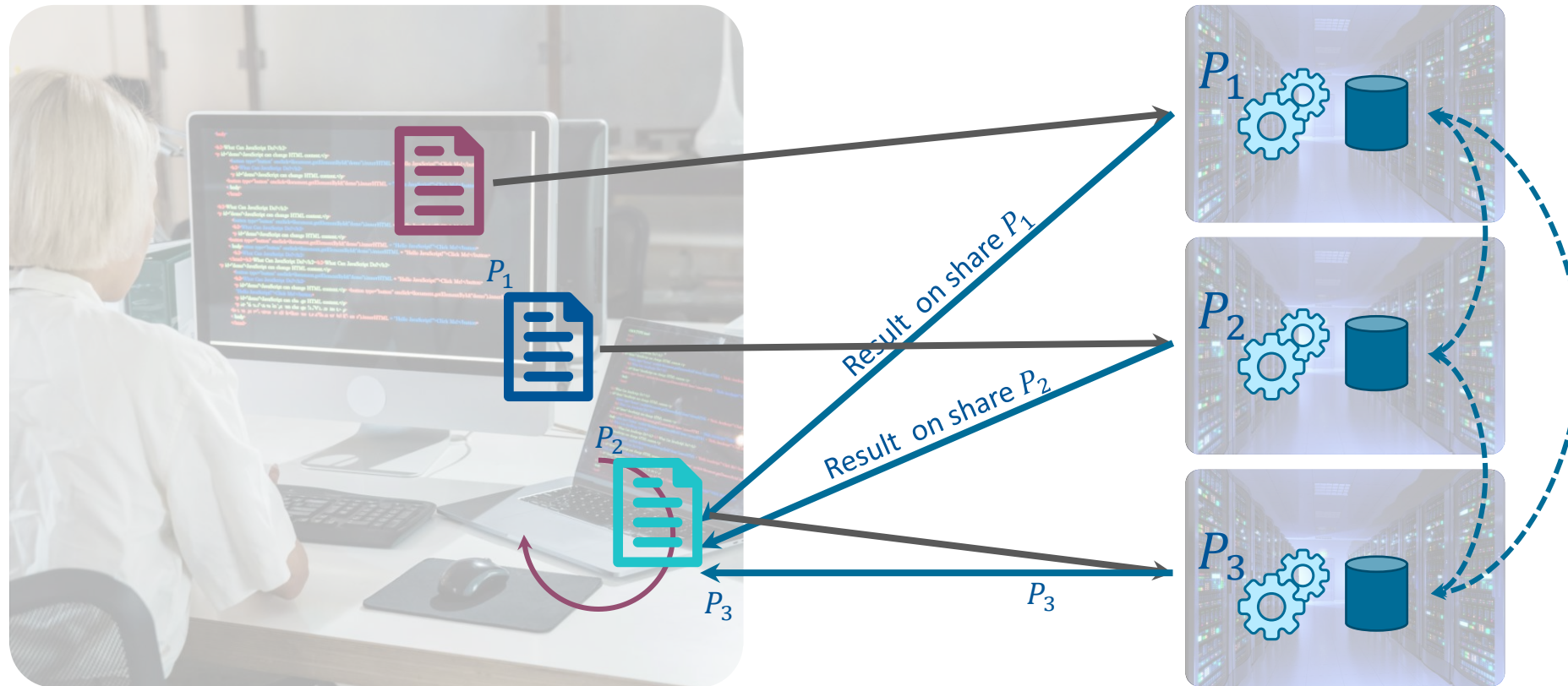


$$x \rightarrow (x_1, x_2, x_3) \quad x_1 + x_2 + x_3 = x$$

MPC deployment example

Client

Shared computing infrastructures



Advantages and limits of MPC

Pros

-
-
-
-
-

Cons

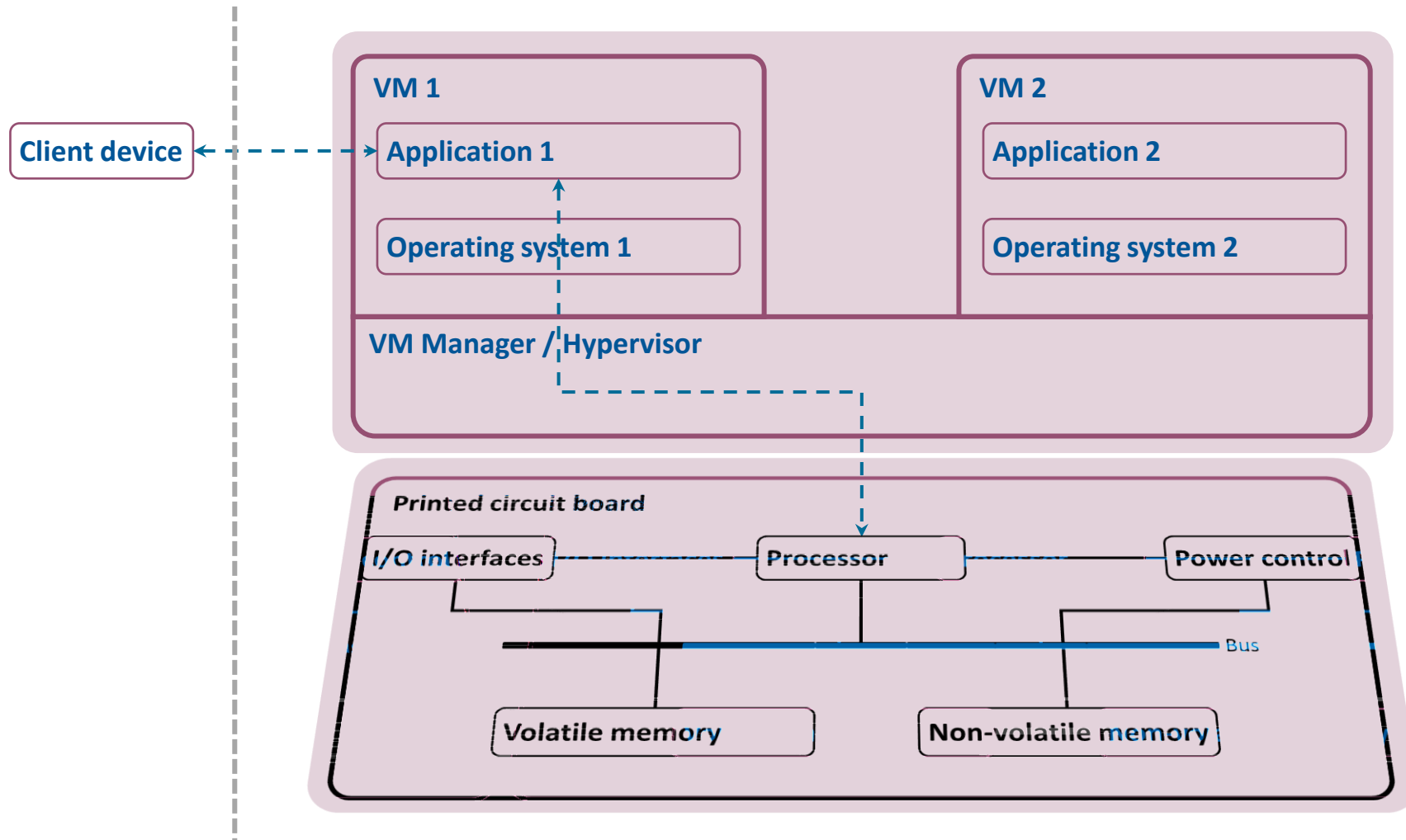
-
-
-
-
-

Trusted execution environments (TEE)

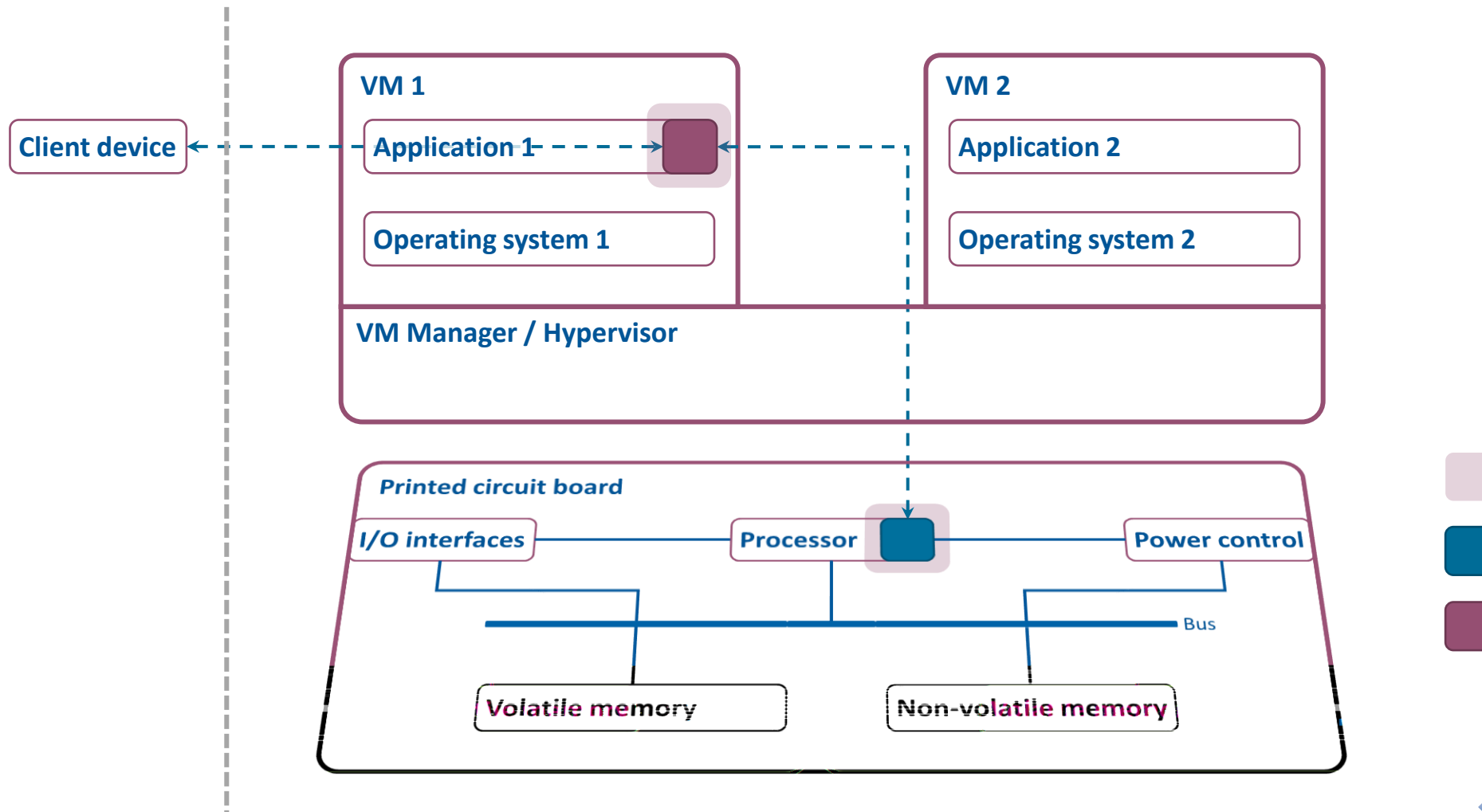
Hardware-based isolated execution

- Technical goal
- Rational
- Requirements
 -
 -
 -
 -

Generic architecture



Possible generic architecture with secure hardware



Verifying integrity of the system

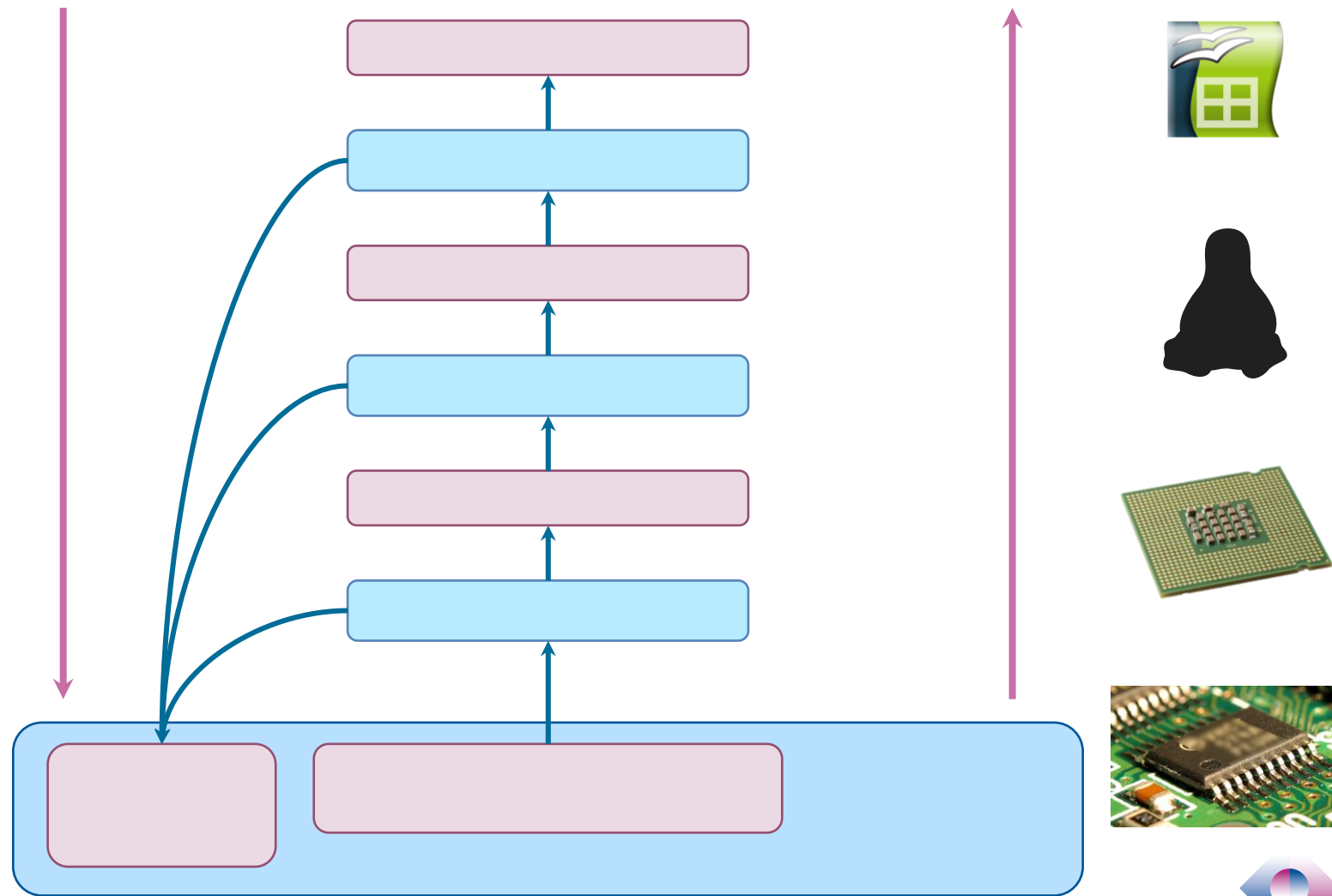
Secure boot

-
-

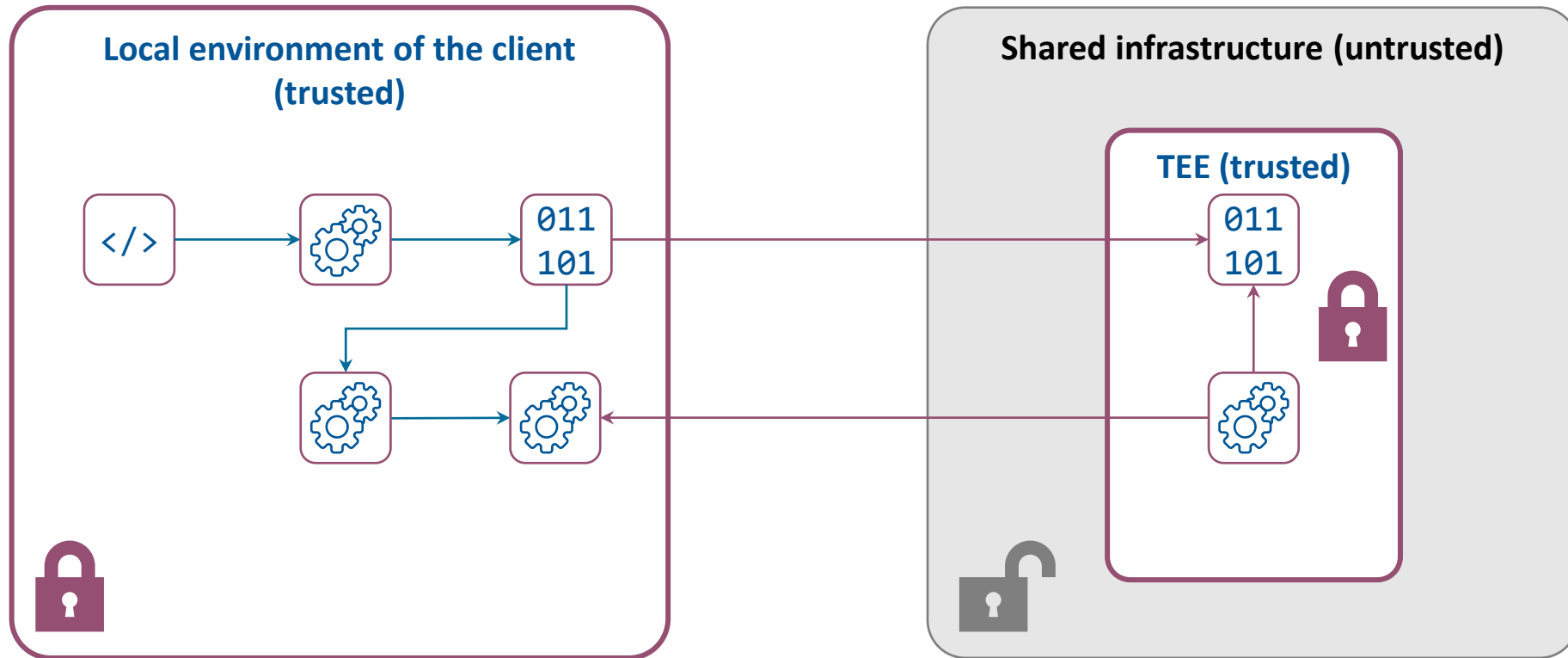
Attestation

-
-
-

Secure booting sequence example



Attestation example



Advantages and limits of TEE

Pros

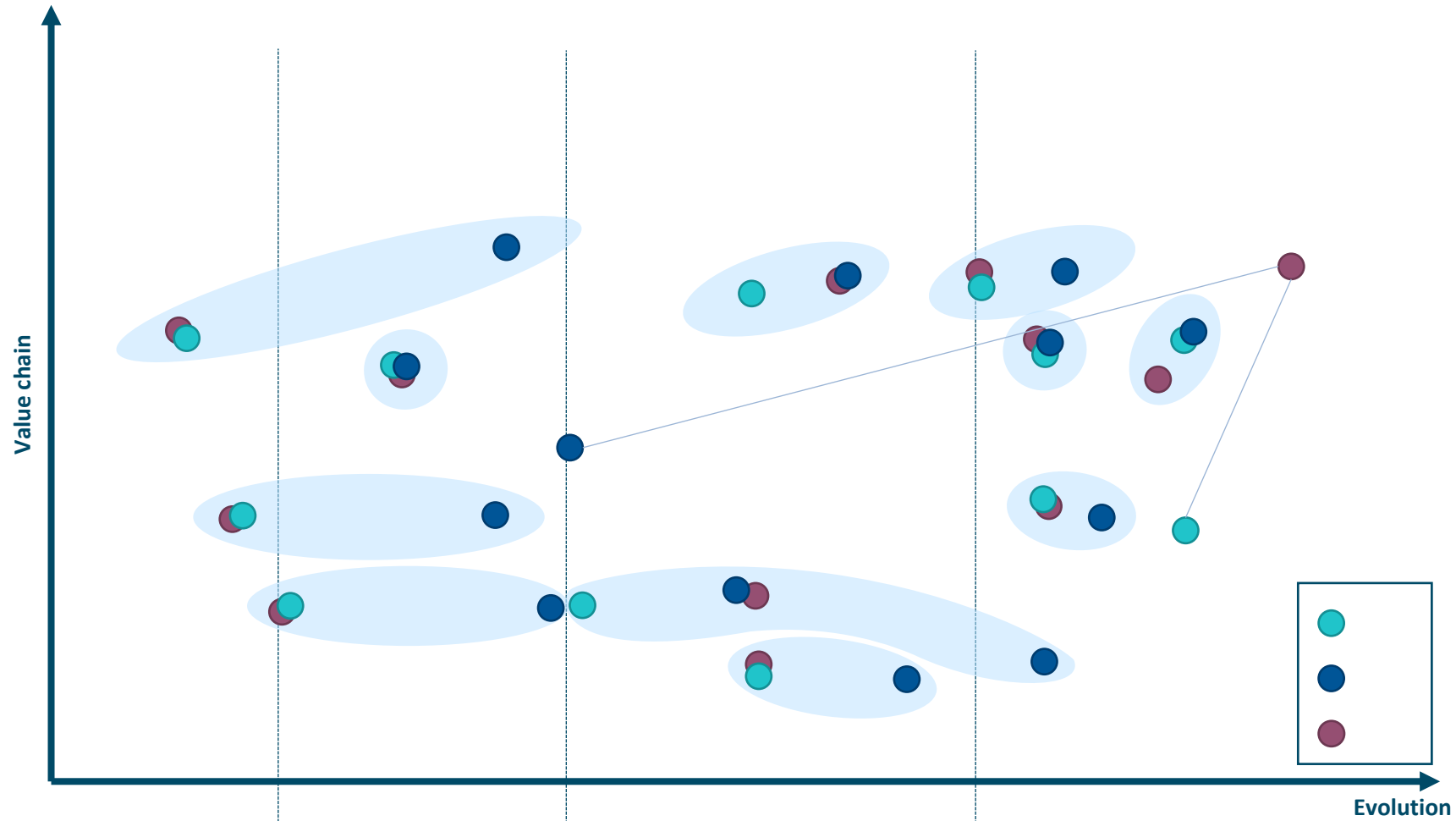
-
-
-

Cons

-
-
-
-

HE, MPC, TEE – Which maturity?

Maturity of confidential computing technologies



TEE-based market offer

AMD SEV-SNP, Intel SGX / TDX

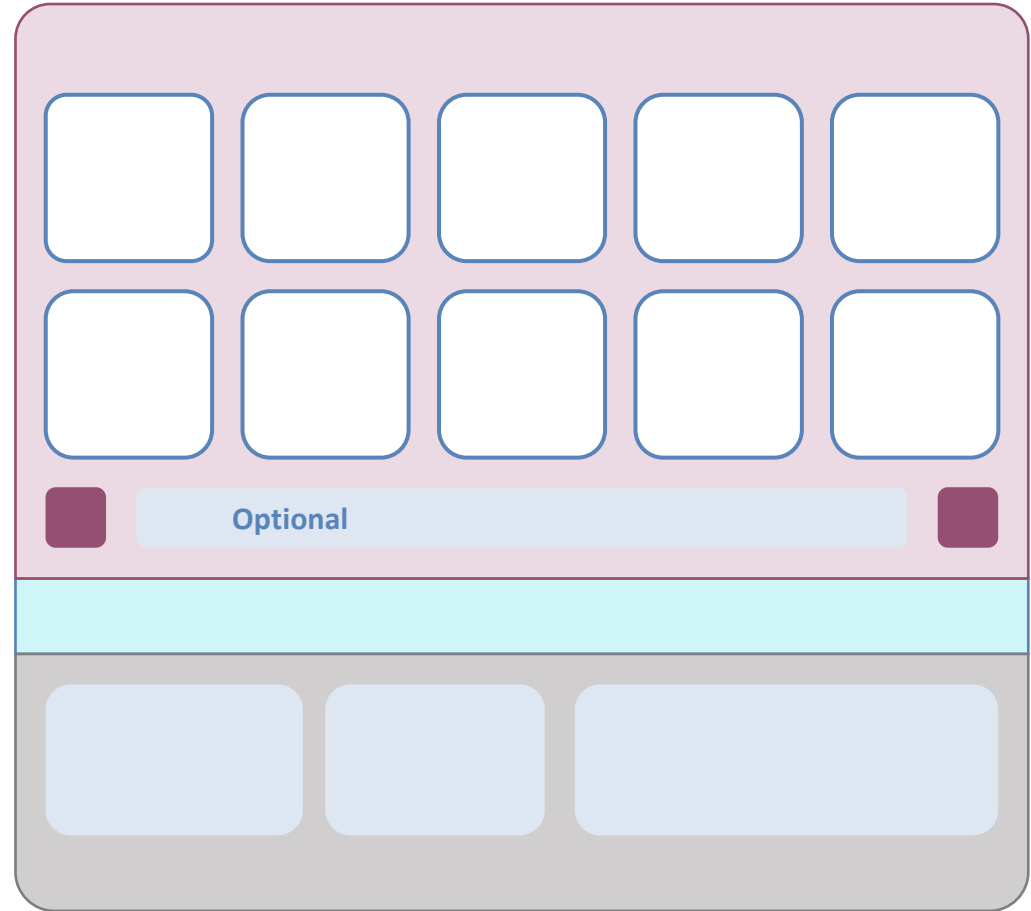
AWS Nitro and Microsoft Azure

Confidential computing on Azure

- -
 - -
 -
 - -
 - -
 - -
- -
 - -
- Microsoft Azure Attestation*
→

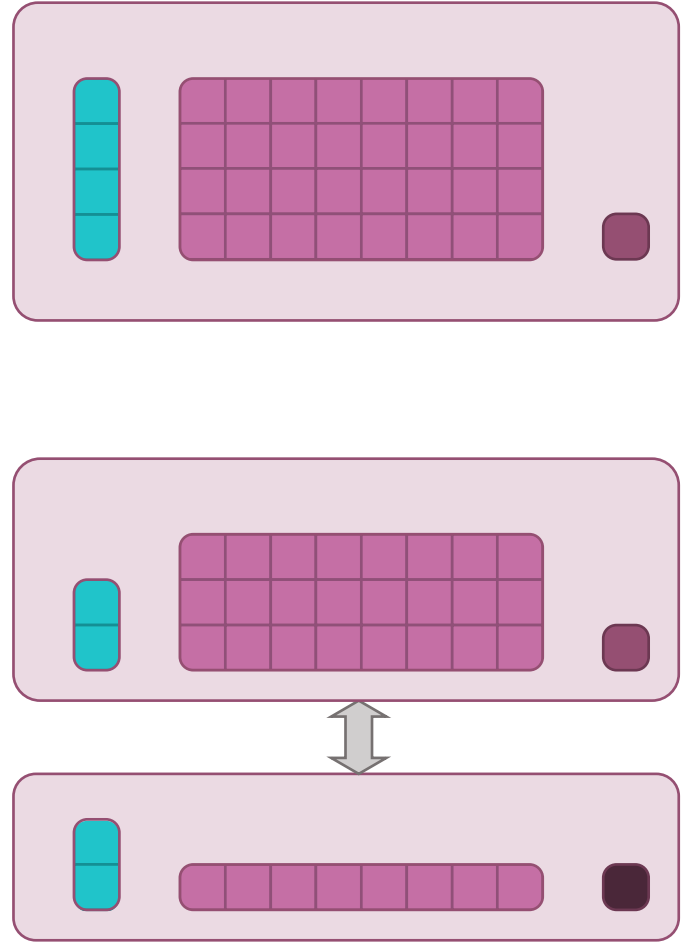
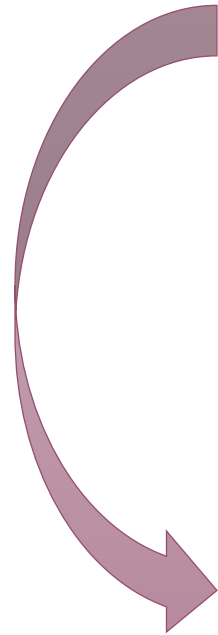
AWS EC2 with “Nitro” architecture

-
-
-
-



AWS "Nitro Enclave"

-
-
-
-
-
-
-
-
-
-



Initiatives and conclusions

Ongoing initiatives

INAMI

-
-
-
-



Smals

-
-



General remarks

-

-

 -

 -

 -

 -

-

 -

 -

 -

-

 -

-

Recommendations

- **Attestation**

-

- **Transparency**

-

- **Key management**

-

-

- **Training**

-

- **Holistic view**

-

Additional recommendations

- Provider access

-

-

-

- Data disposal

- Vulnerability disclosure

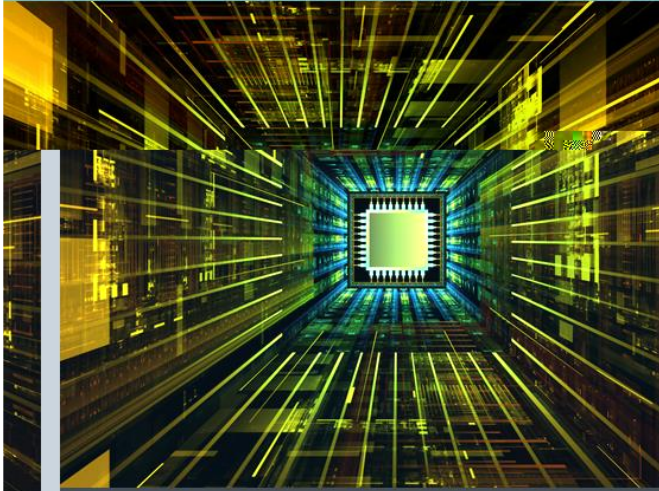
-

Informatieveiligheidscomité Kamer sociale zekerheid en gezondheid
IVC/KSZG/24/114
BERAADSLAGING NR. 24/044 VAN 5 MAART 2024 MET BETREKKING TOT DE GOEDE PRAKTIJKEN DIE TOEGEPAST MOETEN WORDEN BIJ HET GEBRUIK VAN PUBLIEKE CLOUD DIENSTEN
Het informatieveiligheidscomité, kamer sociale zekerheid en gezondheid,
Gelet op de Verordening (EU) nr. 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene Verordening Gegevensbescherming of AVG);
Gelet op de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens;

Comité de sécurité de l'information Chambre sécurité sociale et santé
CSI/CSSS/24/114
DÉLIBÉRATION N° 24/044 DU 5 MARS 2024 RELATIVE AUX BONNES PRATIQUES À APPLIQUER EN CAS D'UTILISATION DE SERVICES CLOUD PUBLICS
Le Comité de sécurité de l'information, chambre sécurité sociale et santé ;
Vu le Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général relatif à la protection des données ou RGPD);
Vu la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ;
Vu la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de

Further reading...

Smals Research
Smals
ICT for society



Informatique confidentielle

État de l'art

Fabien Petitcolas, PhD

Smals Research

HOME BLOG PUBLICATIONS TOOLS RADAR / PLAN TEAM ABOUT

Introduction à l'informatique confidentielle

Posted on 28/02/2023 by Fabien A. P. Petitcolas

On considère généralement que les données peuvent être dans trois états. Celles stockées, par exemple sur un disque dur ou dans une base de données, sont dites « au repos », celles envoyées d'un ordinateur à un autre, par exemple via un réseau, sont « en mouvement, » et les données traitées par le microprocesseur sont « en cours d'utilisation ».

Aujourd'hui, des primitives cryptographiques sont largement déployées pour protéger les données dans les deux premiers états, assurant intégrité et confidentialité. Cependant, le renforcement des réglementations sur la protection des données et de la vie privée et l'augmentation des cyber-menaces de longue durée a fait naître le besoin de protéger les données en cours d'utilisation.

Malheureusement cette protection des données en cours d'utilisation reste difficile, en particulier dans le contexte d'**infrastructures informatiques partagées** : il s'agit en effet d'exécuter un logiciel avec certaines garanties de sécurité sur un ordinateur distant qui peut être détenu et géré par une partie non fiable voire

Pour répondre à la demande de leurs clients traitant des données sensibles ou attirer de nouveaux clients, les fournisseurs d'infrastructures informatiques publiques mettent d'importants moyens en œuvre afin d'améliorer leur sécurité et notamment de mieux protéger les données de leurs clients. Microsoft, par exemple, déclare investir environ un milliard de dollars chaque année dans la sécurité de ses infrastructures [1]. Depuis le milieu des années 2010, ces fournisseurs d'infrastructures investissent notamment dans une offre d'informatique confidentielle. Principalement basée sur des environnements d'exécution de confiance (« *Trusted Execution Environments (TEE)* »), celle-ci permet en principe de réduire la confiance accordée par le client au fournisseur d'infrastructure.

Dans un article précédent, nous avons présenté de manière générale ce qu'étaient ces TEE et leur utilité. Dans cet article nous regardons plus en détail le fonctionnement des principales mises en œuvre commerciales. Cependant, il convient de garder à l'esprit que les définitions d'informatique confidentielle et de

Newsletters & info sessions

Email:

Your email address

Language Dutch French

Last documents

- Quick Review : H2O LLMstudio - Une interface no-code pour le réglage fin des grands modèles de langage (2024/01 - Katy Fokou)
- Quick Review 115: LangChain - LLM application development framework (2023/12 - Bert Vanhalst)
- Quick Review : QR Graphyfic - Interface graphique pour Graph Database (2023/12 - Vandy Berlien)

Smals Research

HOME BLOG PUBLICATIONS TOOLS RADAR / PLAN TEAM ABOUT

Outils pour l'informatique confidentielle

Posted on 24/07/2023 by Fabien A. P. Petitcolas

Nederlandstalige versie

Pour répondre à la demande de leurs clients traitant des données sensibles ou attirer de nouveaux clients, les fournisseurs d'infrastructures informatiques publiques mettent d'importants moyens en œuvre afin d'améliorer leur sécurité et notamment de mieux protéger les données de leurs clients. Microsoft, par exemple, déclare investir environ un milliard de dollars chaque année dans la sécurité de ses infrastructures [1]. Depuis le milieu des années 2010, ces fournisseurs

Newsletters & info sessions

Email:

Your email address

Language Dutch French

Last documents

- Quick Review : H2O LLMstudio - Une interface no-code pour le réglage fin des grands modèles de langage (2024/01 - Katy Fokou)
- Quick Review 115: LangChain - LLM application development framework (2023/12 - Bert Vanhalst)

Tools voor confidential computing

Version en français

Om te voldoen aan de eisen van hun klanten die met gevoelige gegevens omgaan, of om nieuwe klanten aan te trekken, verrichten leveranciers van publieke IT- infrastructuur inspanningen om hun beveiliging te verbeteren en met name om de gegevens van hun klanten beter te beschermen. Microsoft, bijvoorbeeld, zegt elk jaar ongeveer een miljard dollar te investeren in de beveiliging van zijn infrastructuur [1]. Sinds halftweg 2010 investeren deze infrastructuurleveranciers in een aanbod van *confidential computing*. Voornamelijk gebaseerd op *Trusted Execution Environments (TEE)*, vermindert dit in principe het vereiste vertrouwen van de klant in de infrastructuurleverancier.

Newsletters & info sessions

Email:

Your email address

Language Dutch French

Last documents

- Quick Review : H2O LLMstudio - Une interface no-code pour le réglage fin des grands modèles de langage (2024/01 - Katy Fokou)
- Quick Review 115: LangChain - LLM application development framework (2023/12 - Bert Vanhalst)