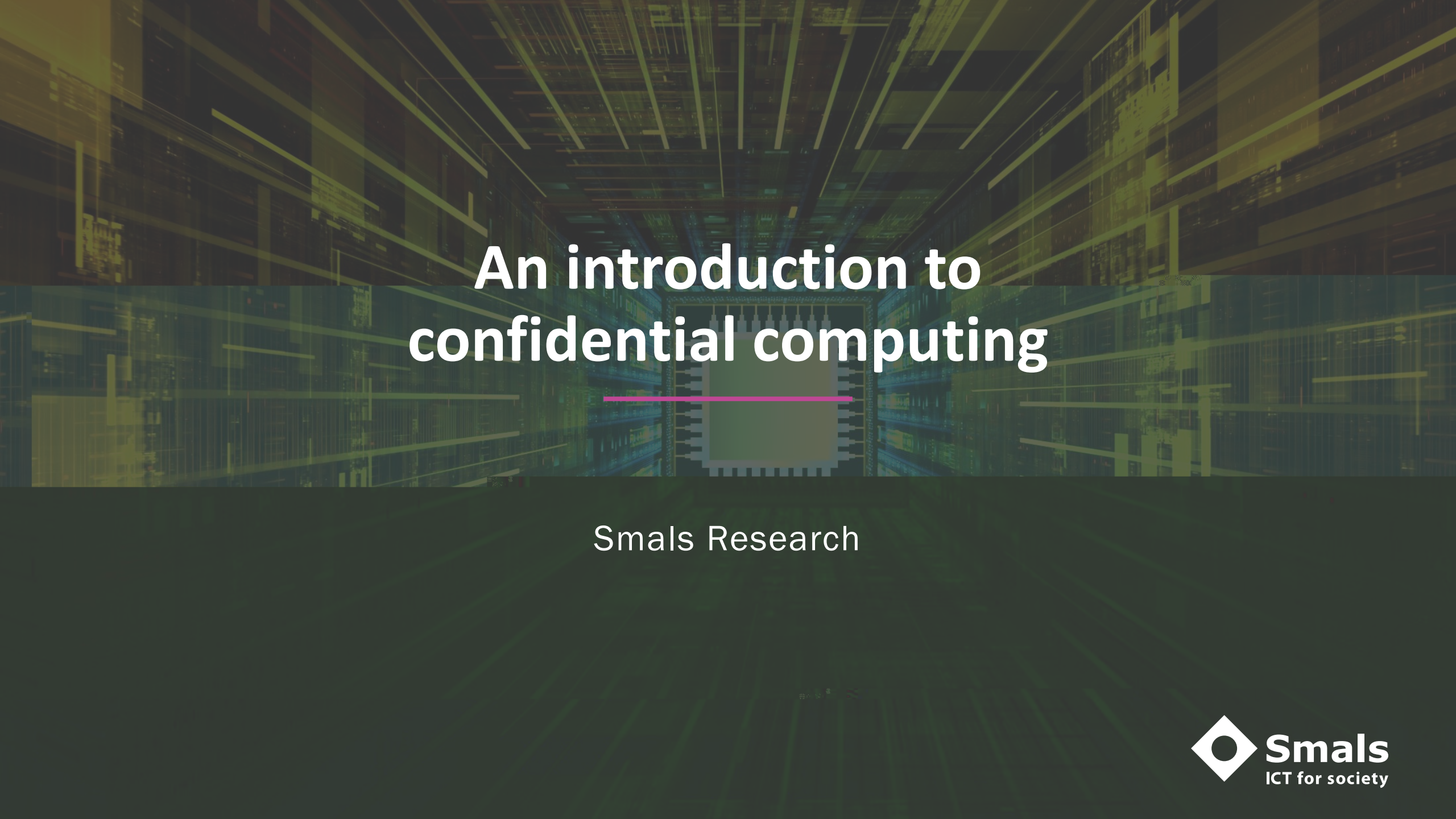


An introduction to confidential computing

Smals Research

Smals
ICT for society

Agenda

General overview

-
-
-
-
-

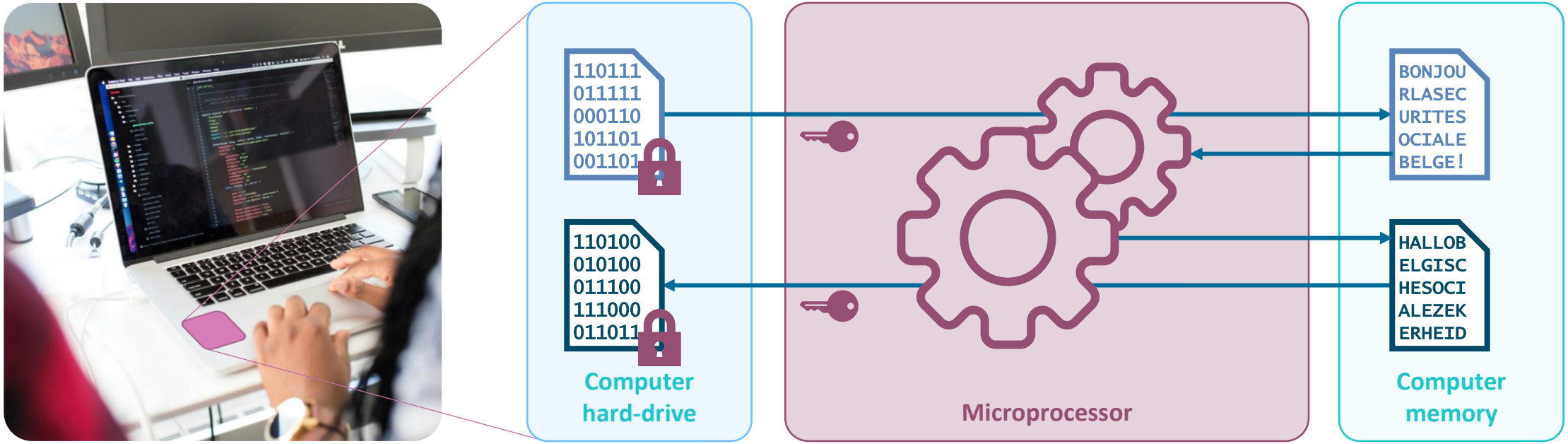
Market offer for TEE

-
-

Conclusions and recommendations

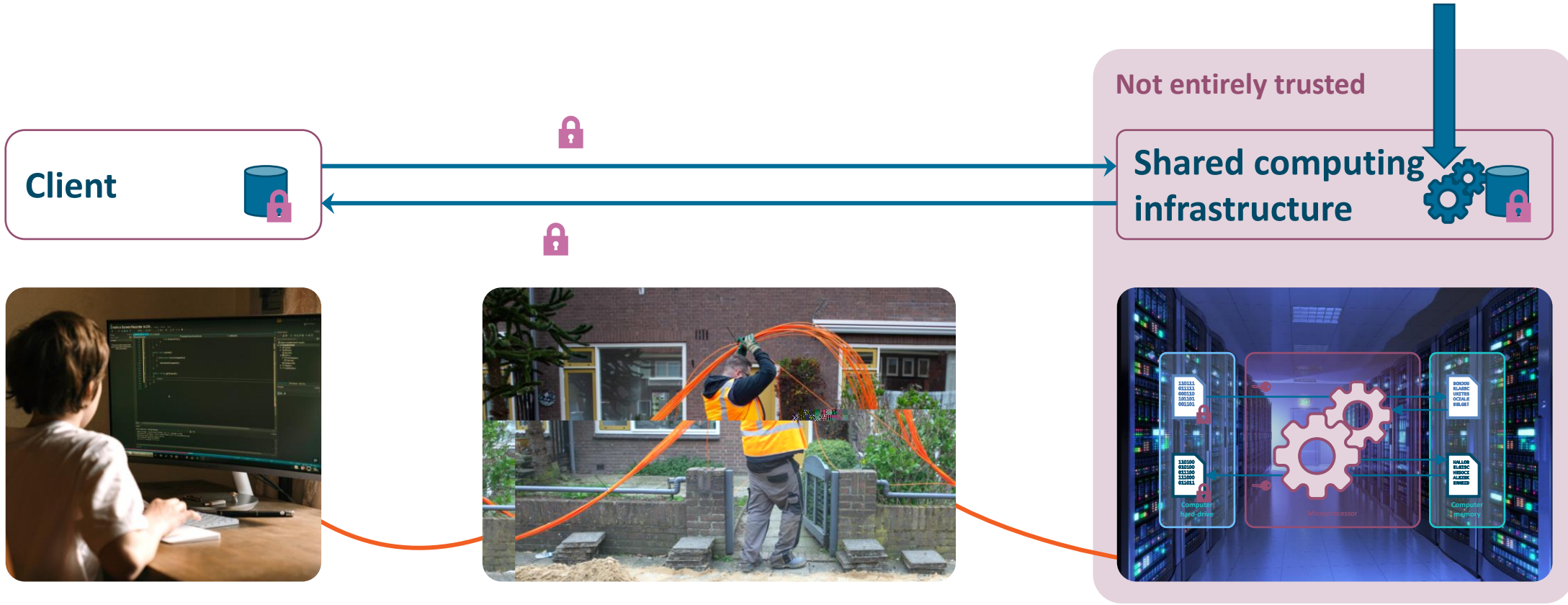
Smals
ICT for society

Traditional computation on encrypted data



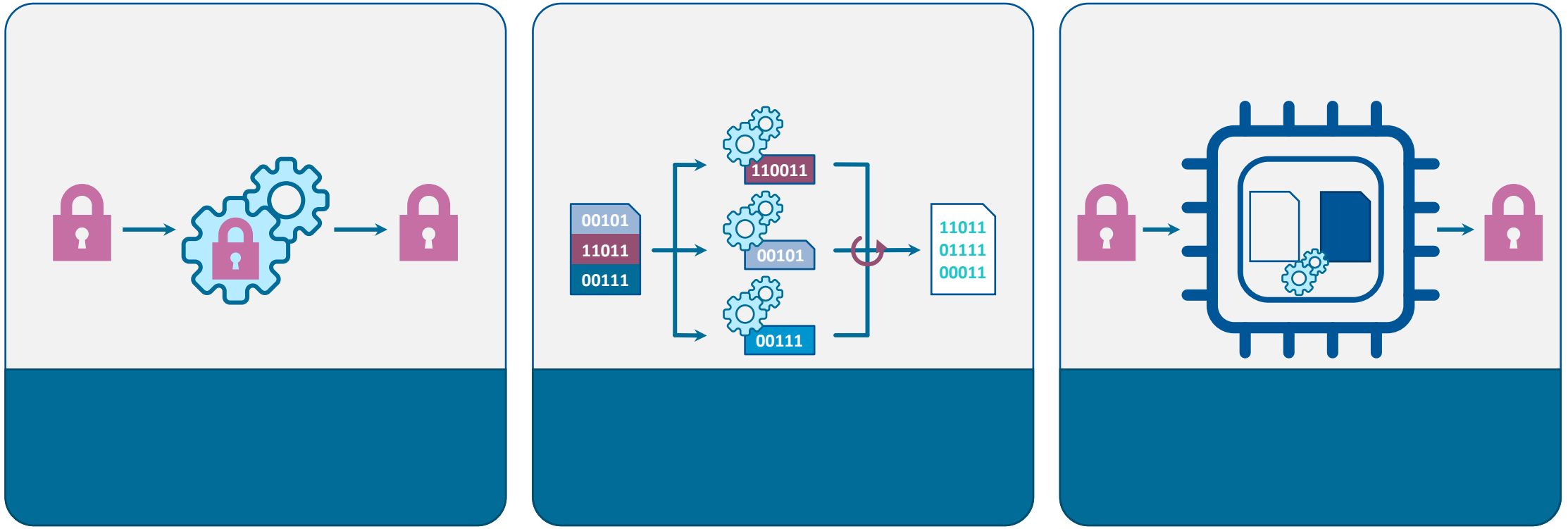
Smals
ICT for society

Basic remote computation



Main techniques for trusted remote computation

Aim: move the infrastructure provider outside of the trust boundary

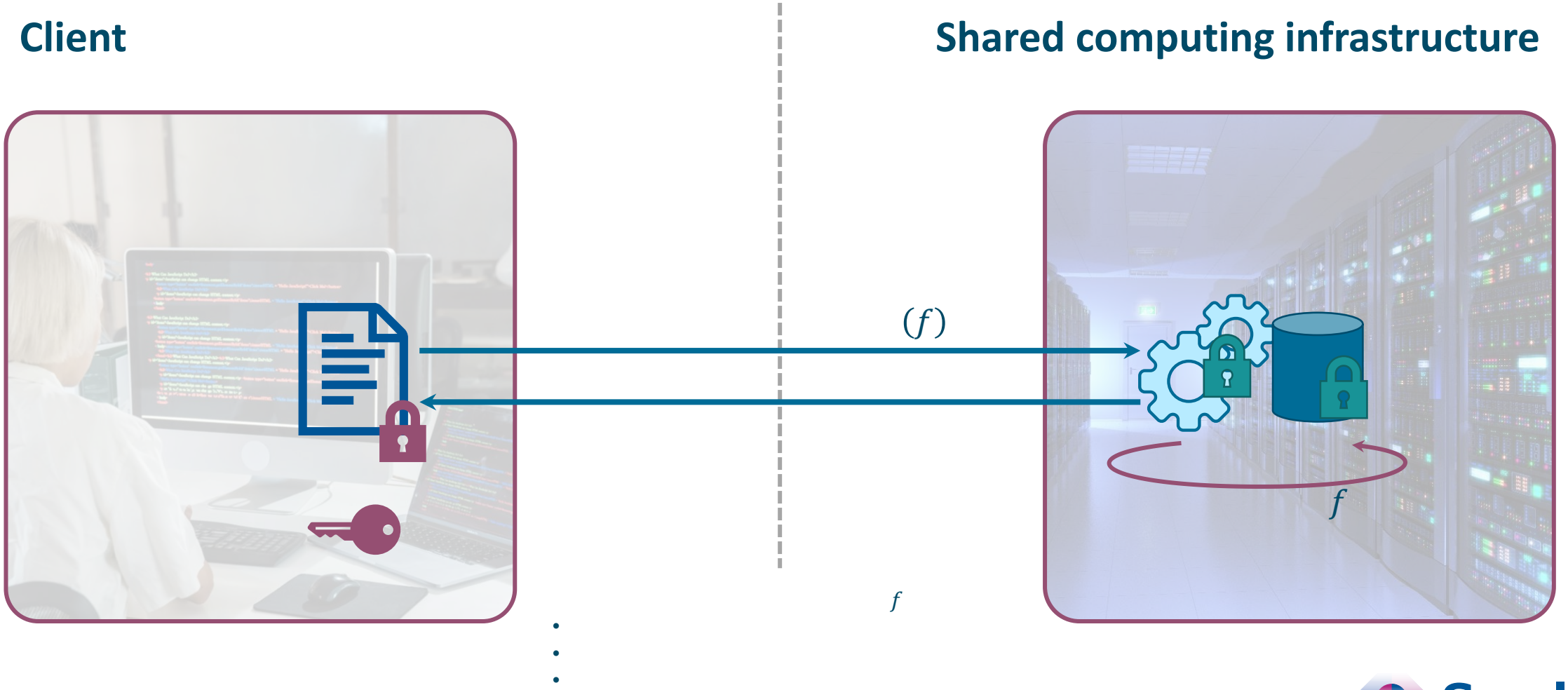


Smals
ICT for society

Homomorphic encryption (HE)

Smals
ICT for society

Homomorphic encryption: schematic overview



Advantages and limits of homomorphic encryption

Pros

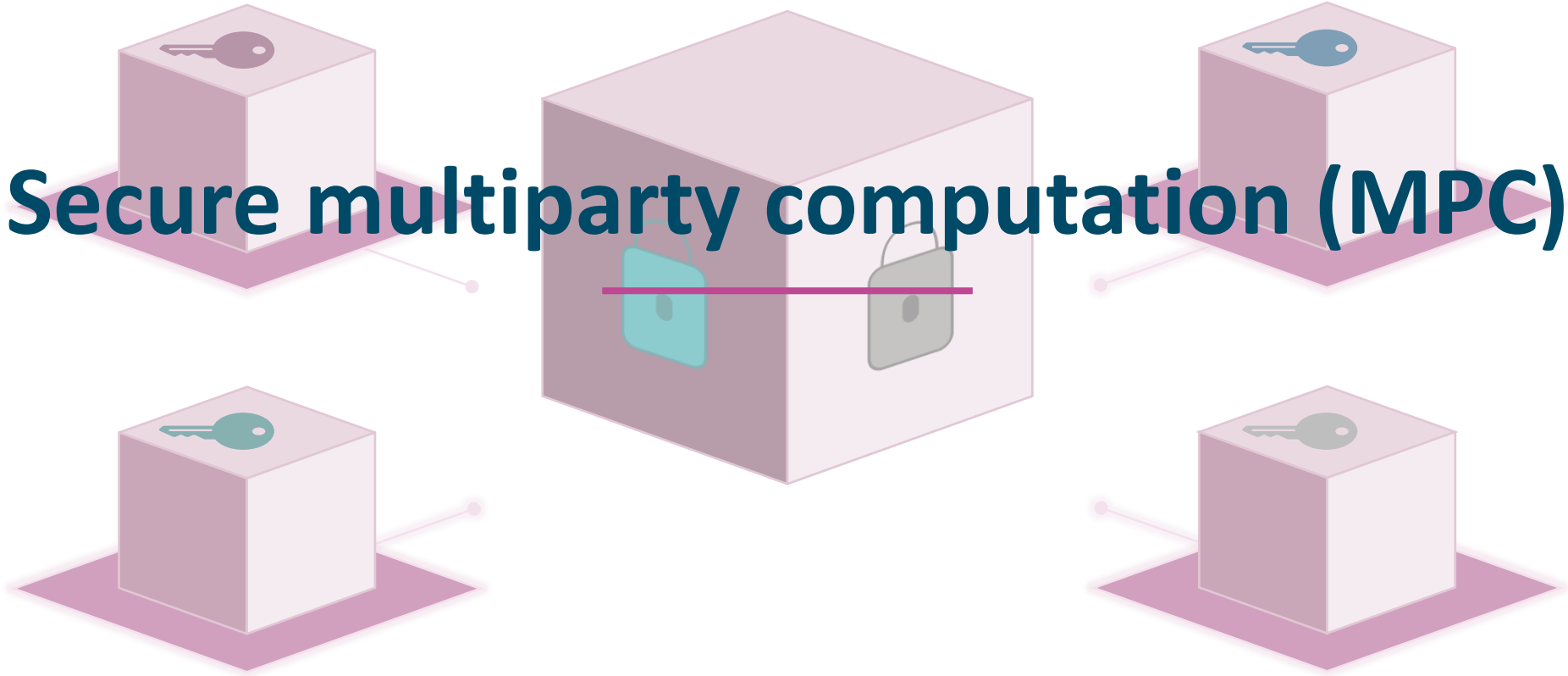
-
-
-
-

Cons

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

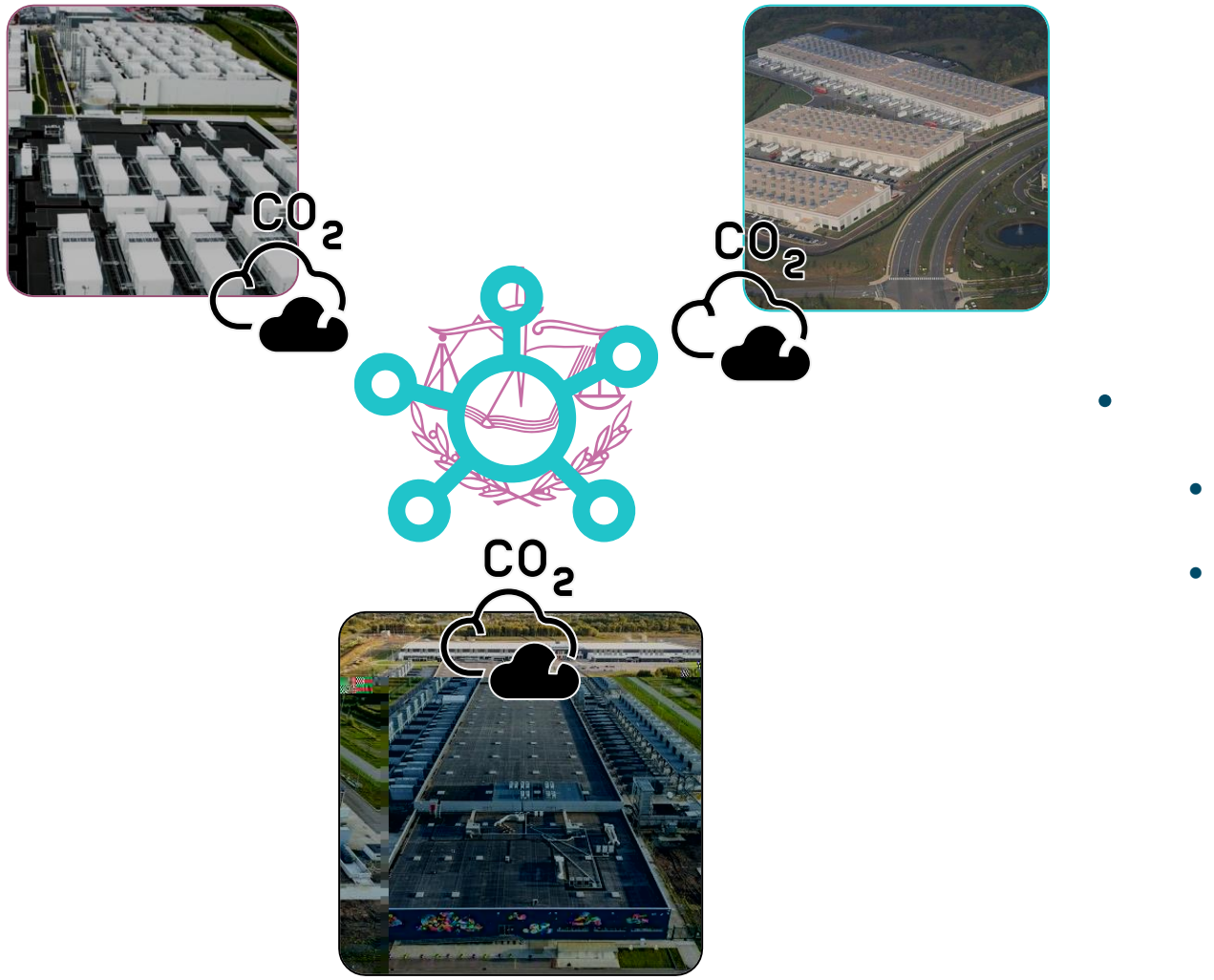
Smals
ICT for society

Secure multiparty computation (MPC)



Smals
ICT for society

MPC problem example

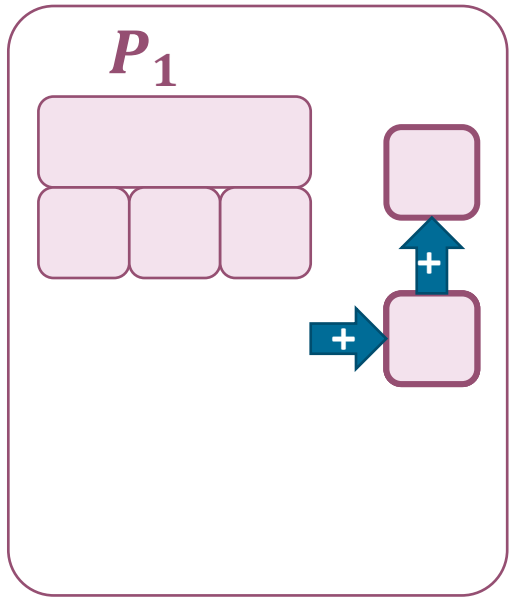


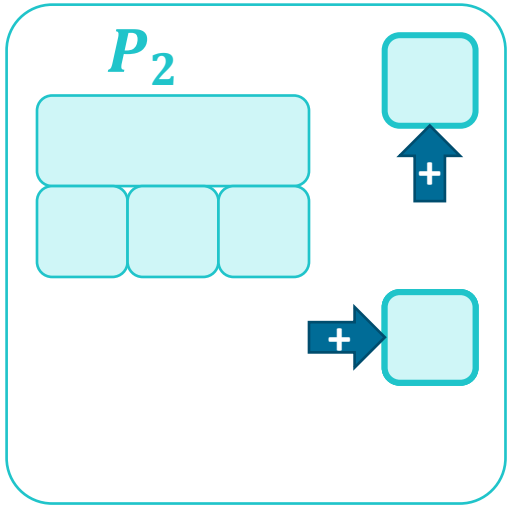
MPC problem and *a* solution

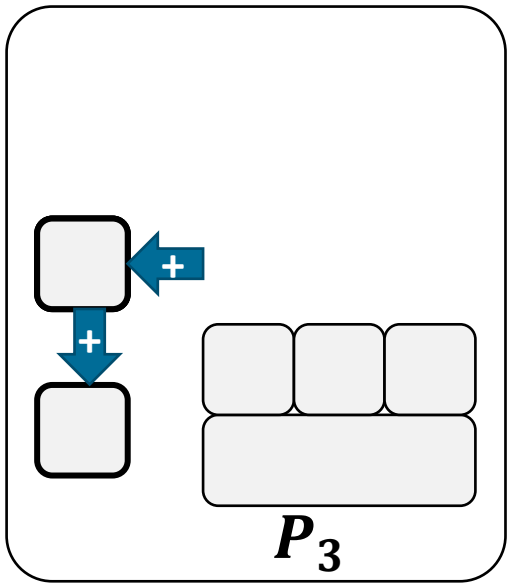
- **Problem** n $P_1, \ldots, P_n$ x_i f
  - $z = f(x_1, \ldots, x_n)$
  - $x_1, \ldots, x_n$
- **MPC solution example**
  - f $+$ $\times$
  -
    -
    -
    -

Smals
ICT for society

MPC in action: simple addition example





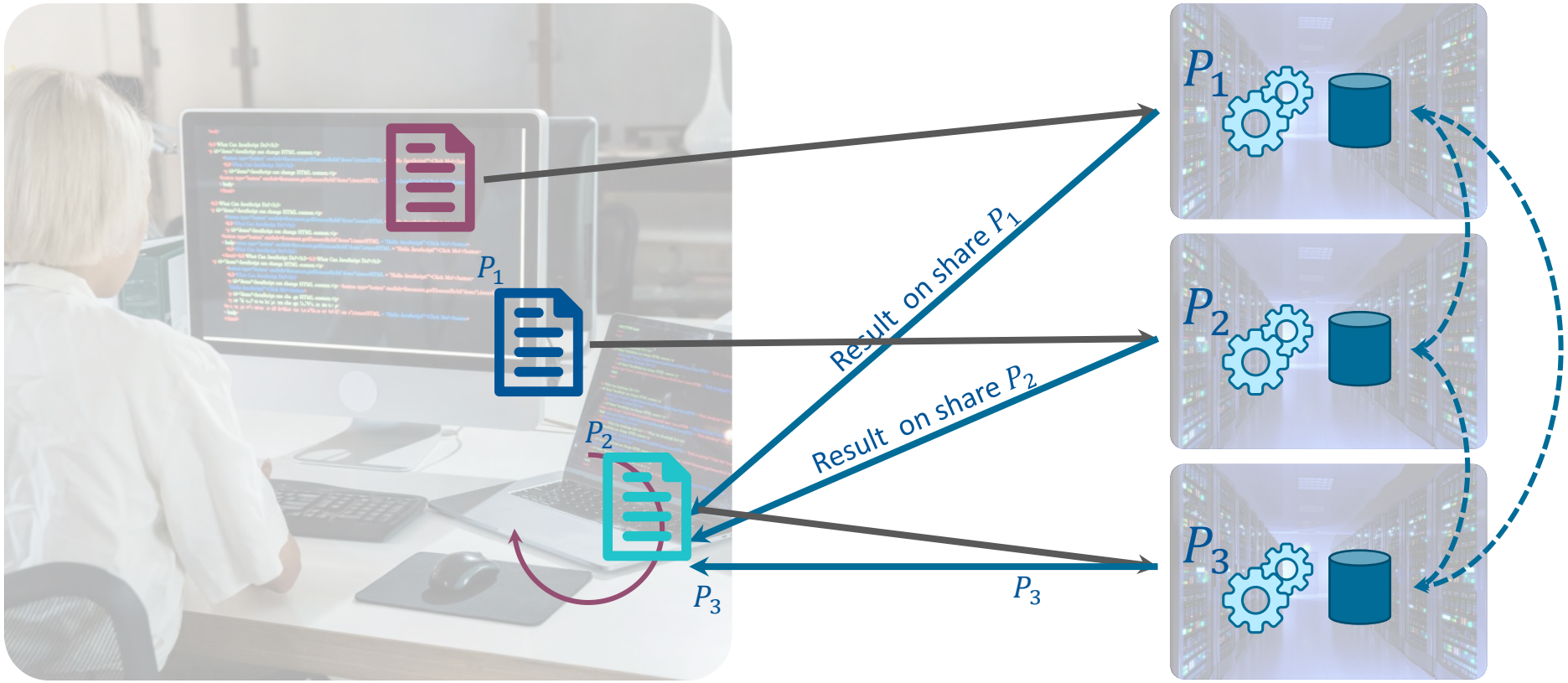


$x \rightarrow (x_1, x_2, x_3)$ $\quad$ $x_1 + x_2 + x_3 = x$

MPC deployment example

Client

Shared computing infrastructures



Smals
ICT for society

Advantages and limits of MPC

Pros	Cons
•	•
•	•
•	•
•	•
•	•

Smals
ICT for society

Trusted execution environments (TEE)

Smals
ICT for society

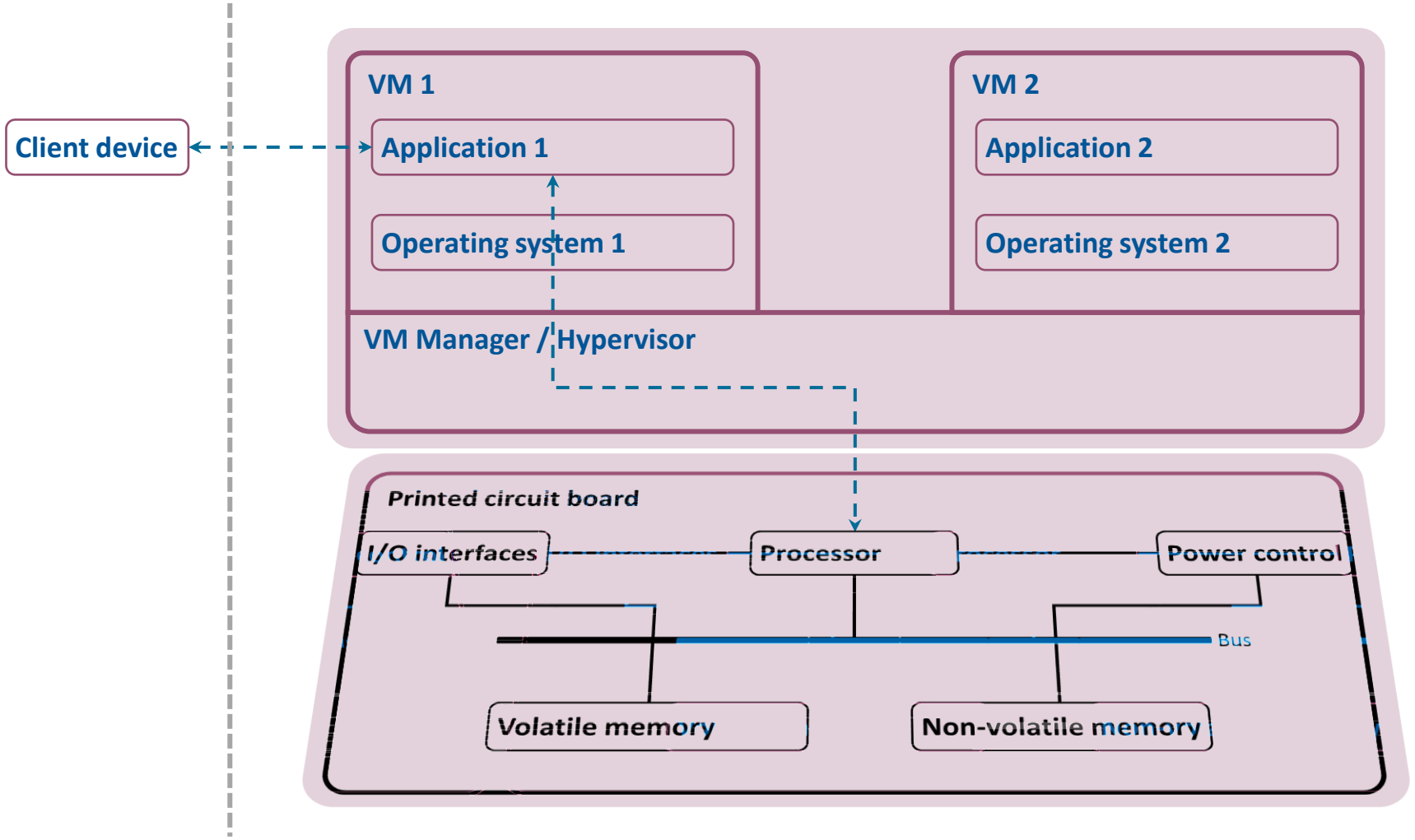
Hardware-based isolated execution

- Technical goal

- Rational
- Requirements
  -
  -
  -
  -

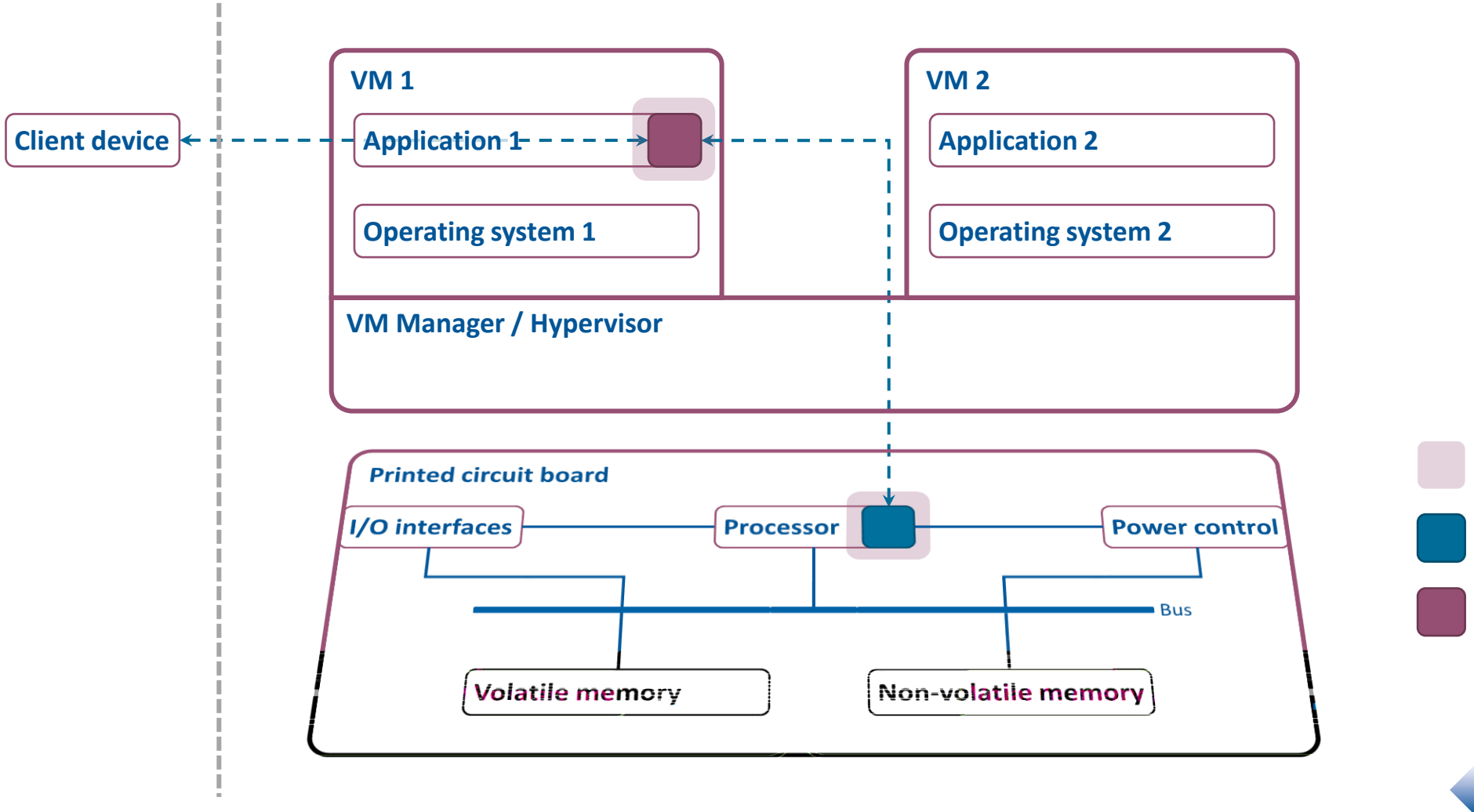
Smals
ICT for society

Generic architecture



Smals
ICT for society

Possible generic architecture with secure hardware



Smals
ICT for society

Verifying integrity of the system

Secure boot

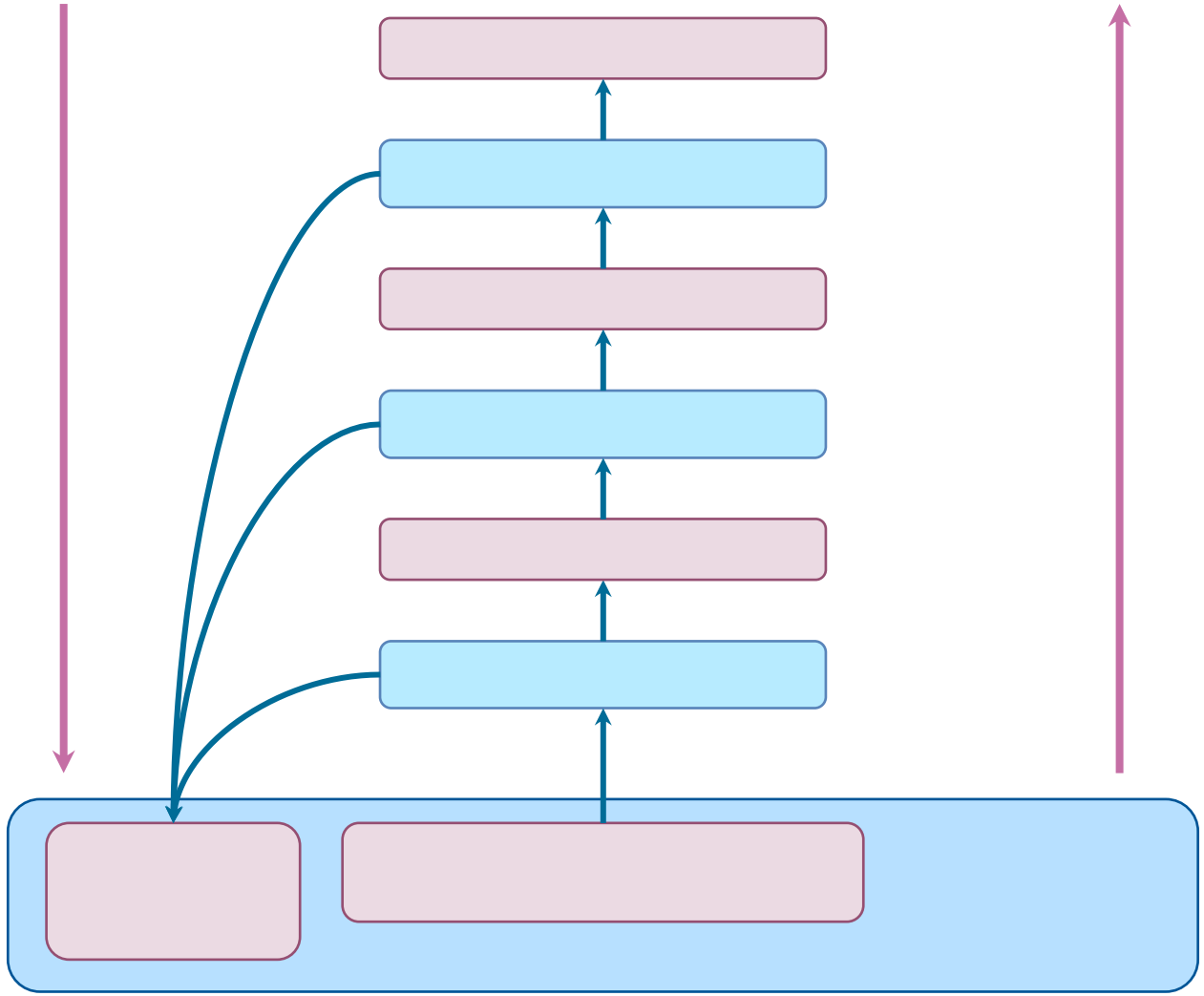
-
-

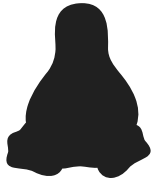
Attestation

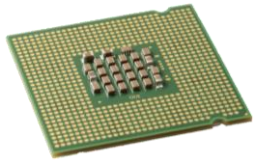
-
-
  -

Smals
ICT for society

Secure booting sequence example

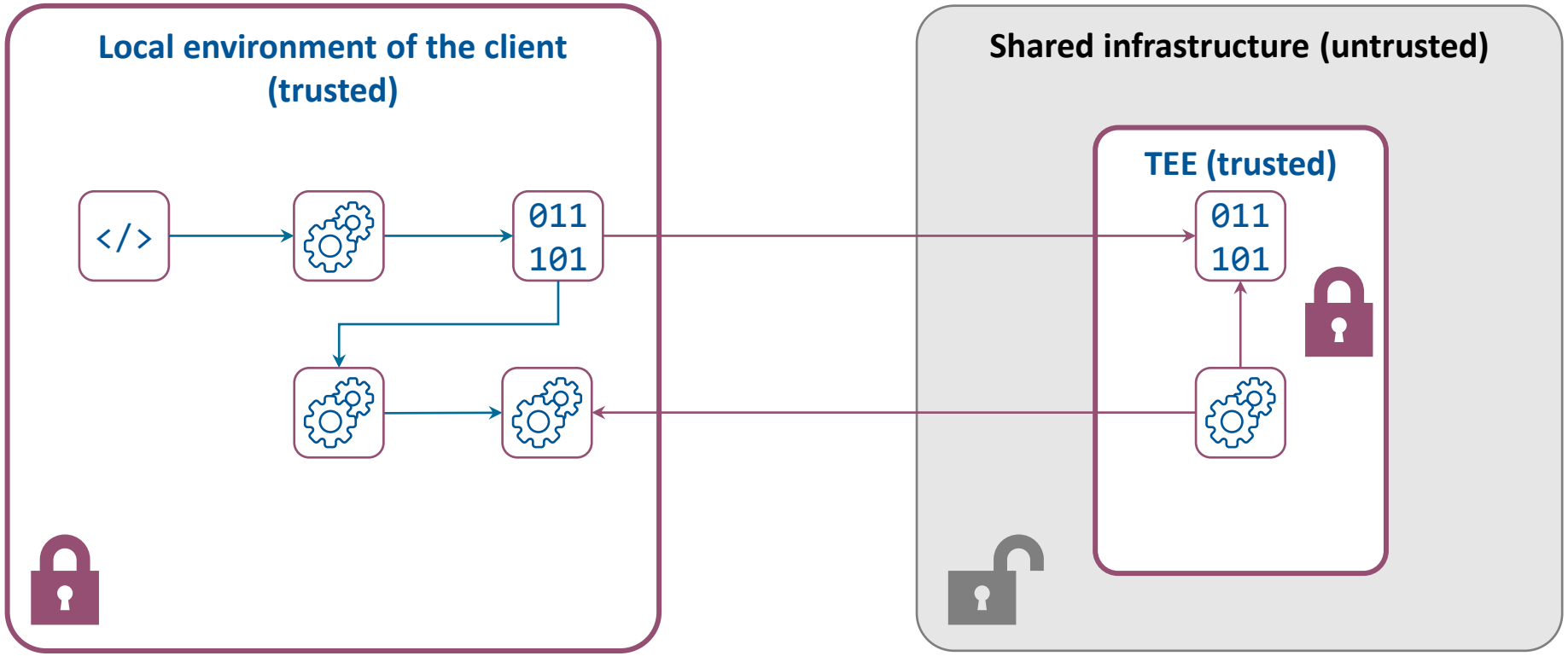






Smals
ICT for society

Attestation example



Advantages and limits of TEE

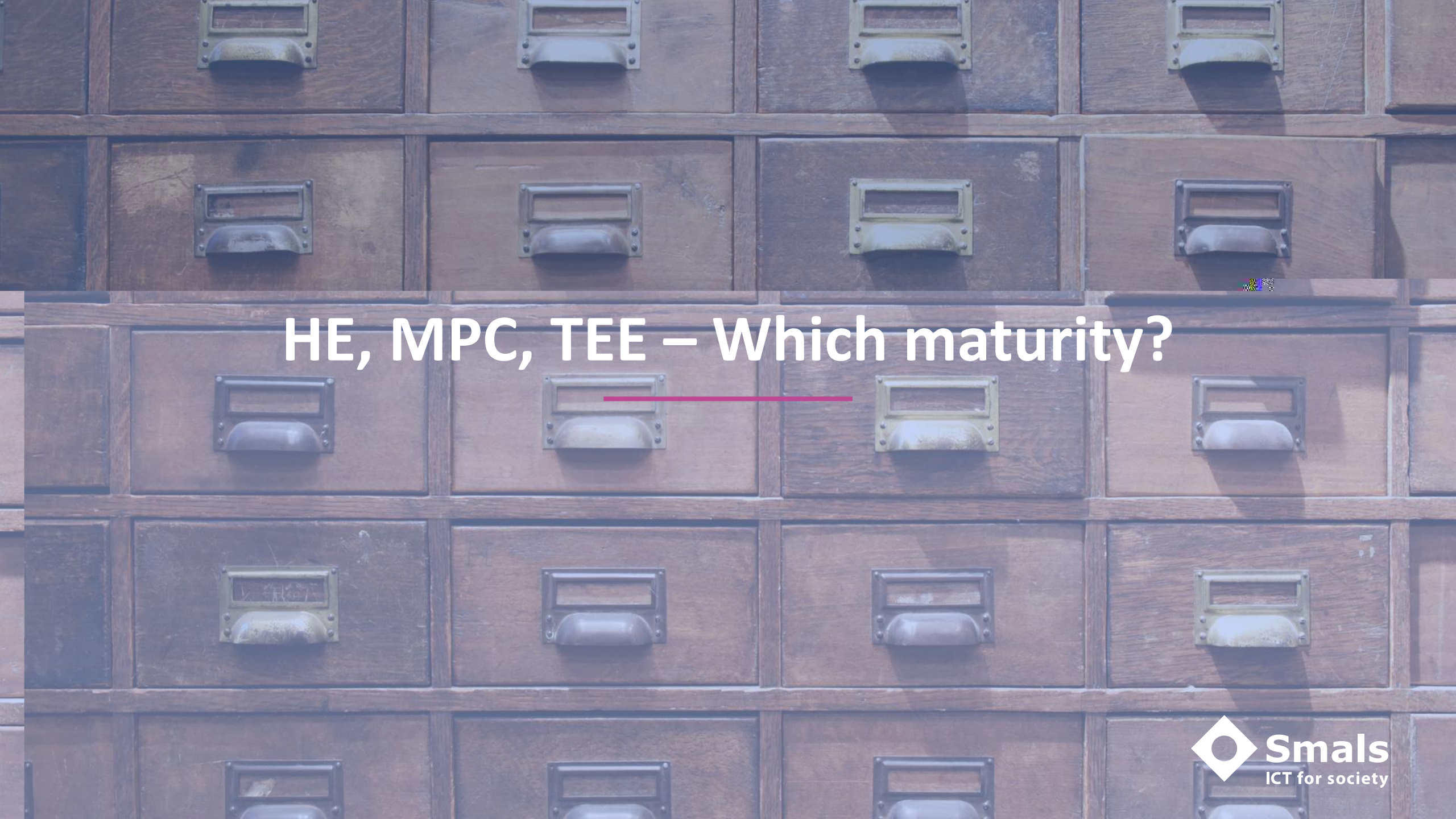
Pros

-
-
-

Cons

-
-
-
-

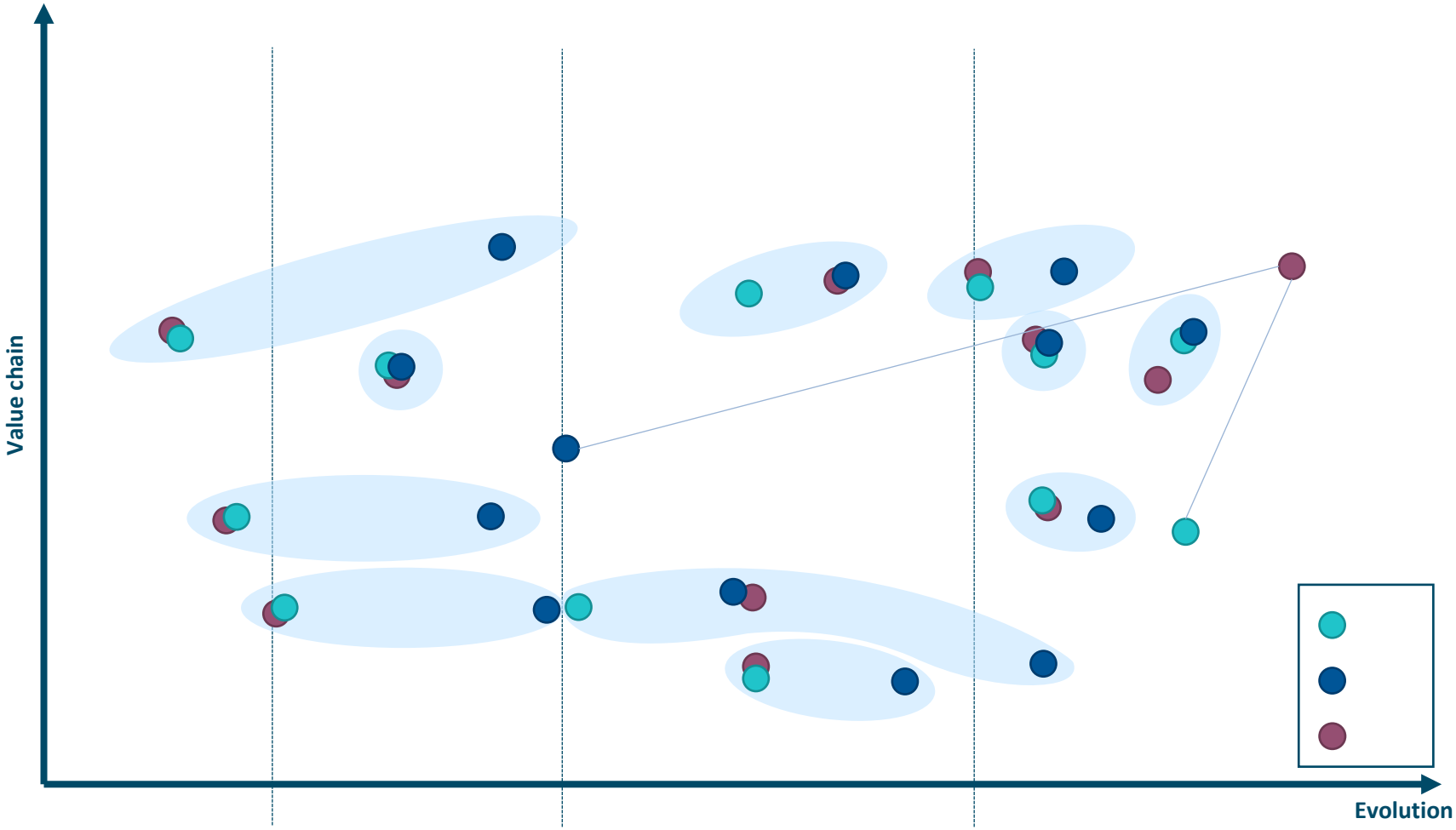
Smals
ICT for society



HE, MPC, TEE – Which maturity?

Smals
ICT for society

Maturity of confidential computing technologies



Smals
ICT for society

TEE-based market offer

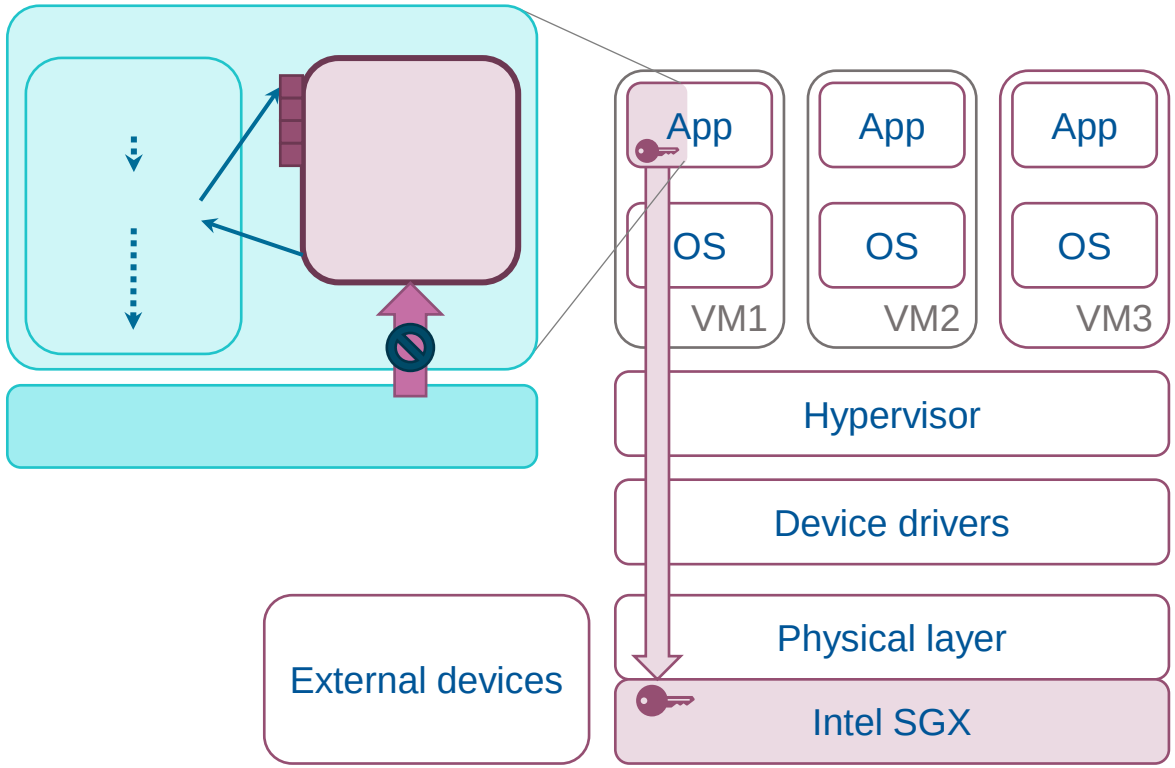
AMD SEV-SNP, Intel SGX / TDX

AWS Nitro and Microsoft Azure

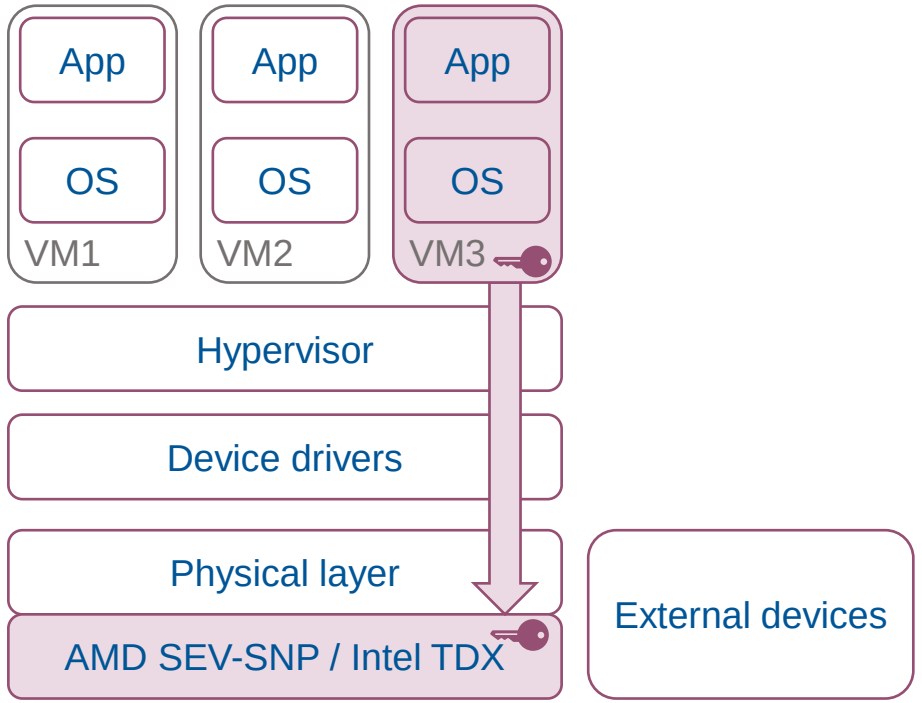
Smals
ICT for society

Two main types of hardware-based isolation

Intel SGX



AMD SEV-SNP, Intel TDX



Untrusted element Trusted element

Smals
ICT for society

Confidential computing on Azure

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

      →
  -
-
  -

Smals
ICT for society

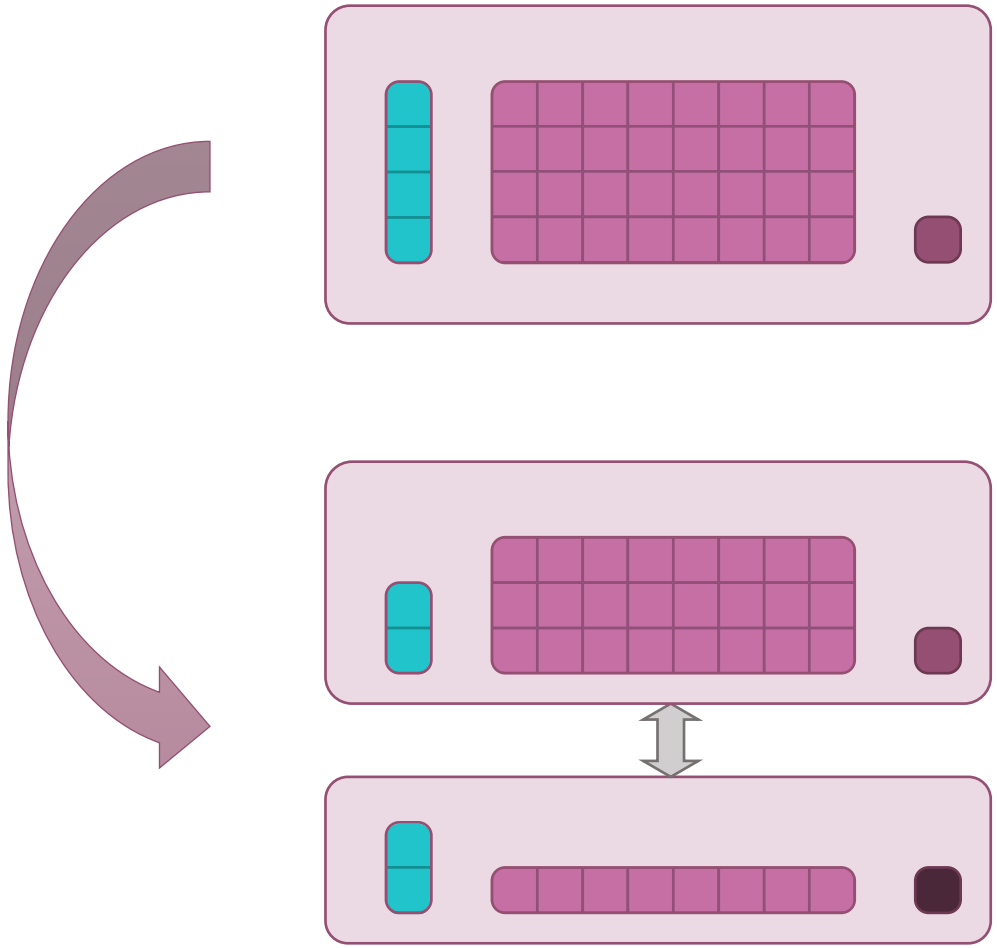
AWS EC2 with “Nitro” architecture

-
  -
  -
  -

Smals
ICT for society

AWS “Nitro Enclave”

-
  -
  -
  -
  -
  -
-
-
-



Initiatives and conclusions

Smals
ICT for society

Ongoing initiatives

INAMI

-
  -
  -
-

Smals

-
-

General remarks

-
-
    -
    -
    -
    -
-
    -
    -
-

Recommendations

- Attestation
  -
- Transparency
  -
- Key management
  -
  -
- Training
  -
- Holistic view
  -

Smals
ICT for society

Additional recommendations

- **Provider access**
  -
  -
  -
- **Data disposal**
- **Vulnerability disclosure**
  -

Informatieveiligheidscomité
Kamer sociale zekerheid en gezondheid

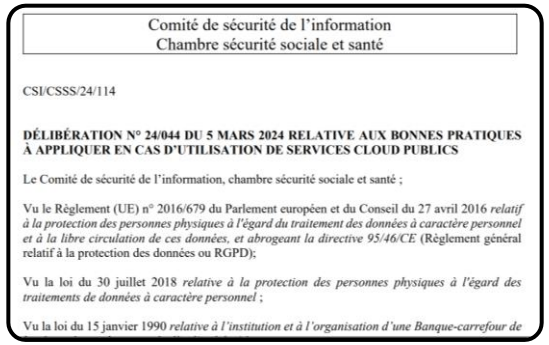
IVC/KSZG/24/114

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 ;

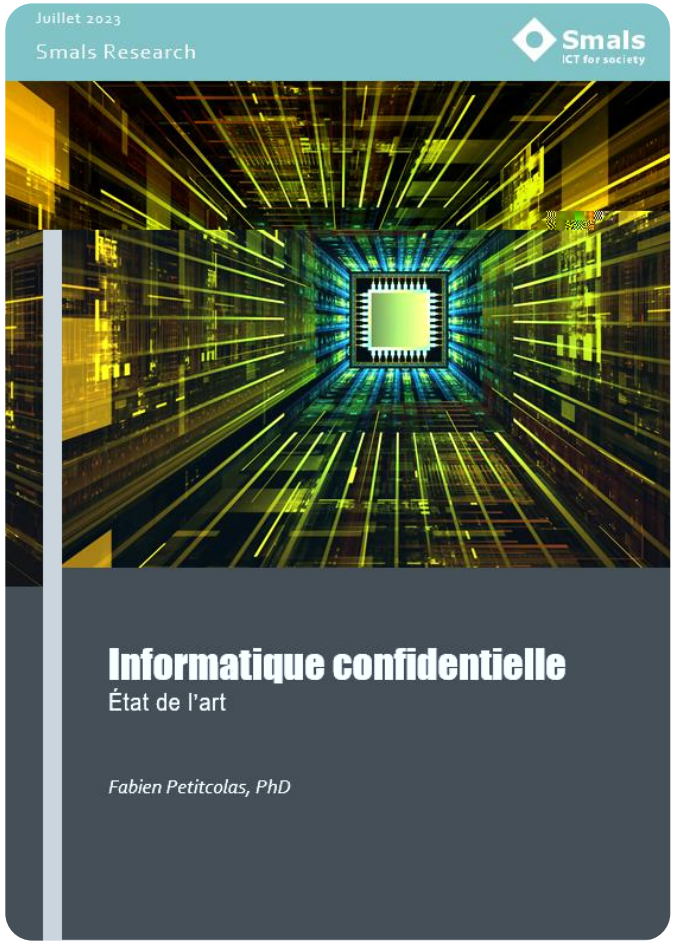
Vu le Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* (Règlement général relatif à la protection des données ou RGPD);

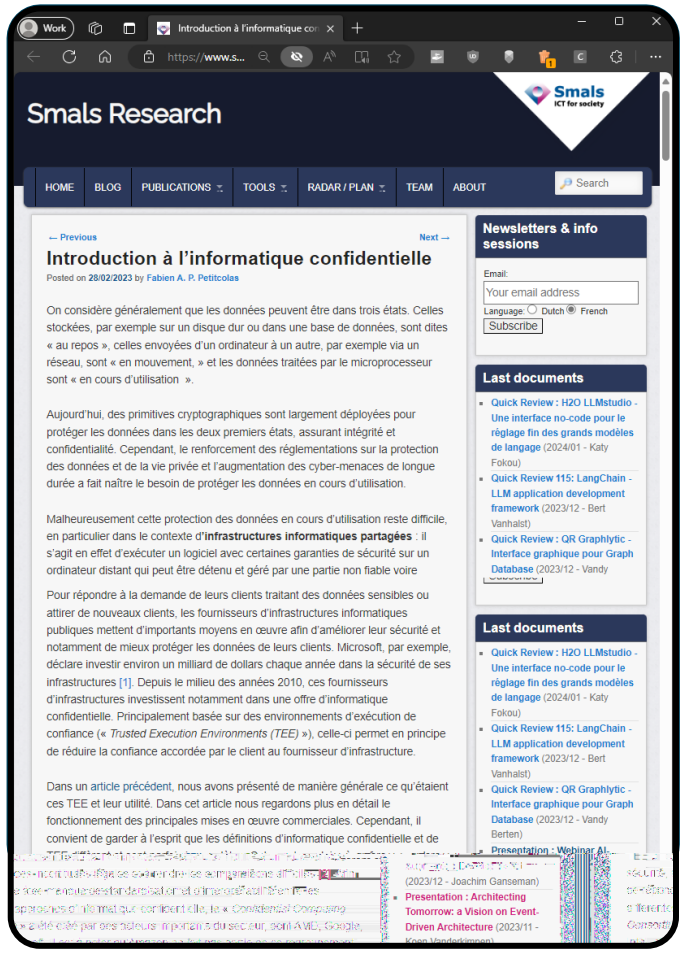
Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* ;

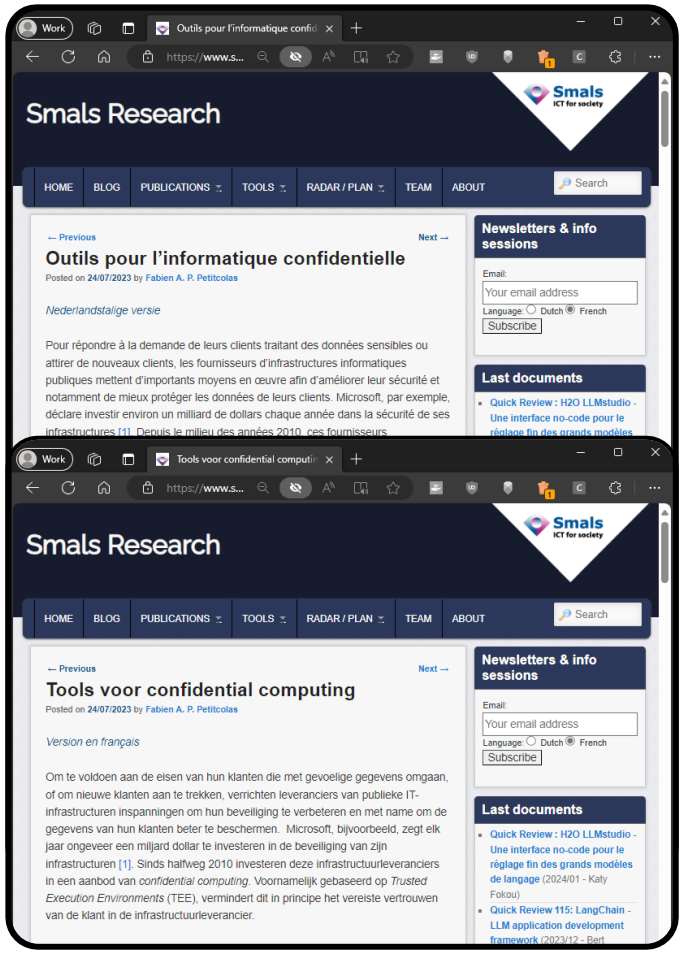
Vu la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de*

Smals
ICT for society

Further reading…







Smals
ICT for society