A reflection on the potential role of MultiParty Computation for the production of (future) Official Statistics

Fabio Ricciato
Unit A5 'Methodology; Innovation in Official Statistics'
Eurostat

MPC DATA PRIVACY SUMMIT
October 2022

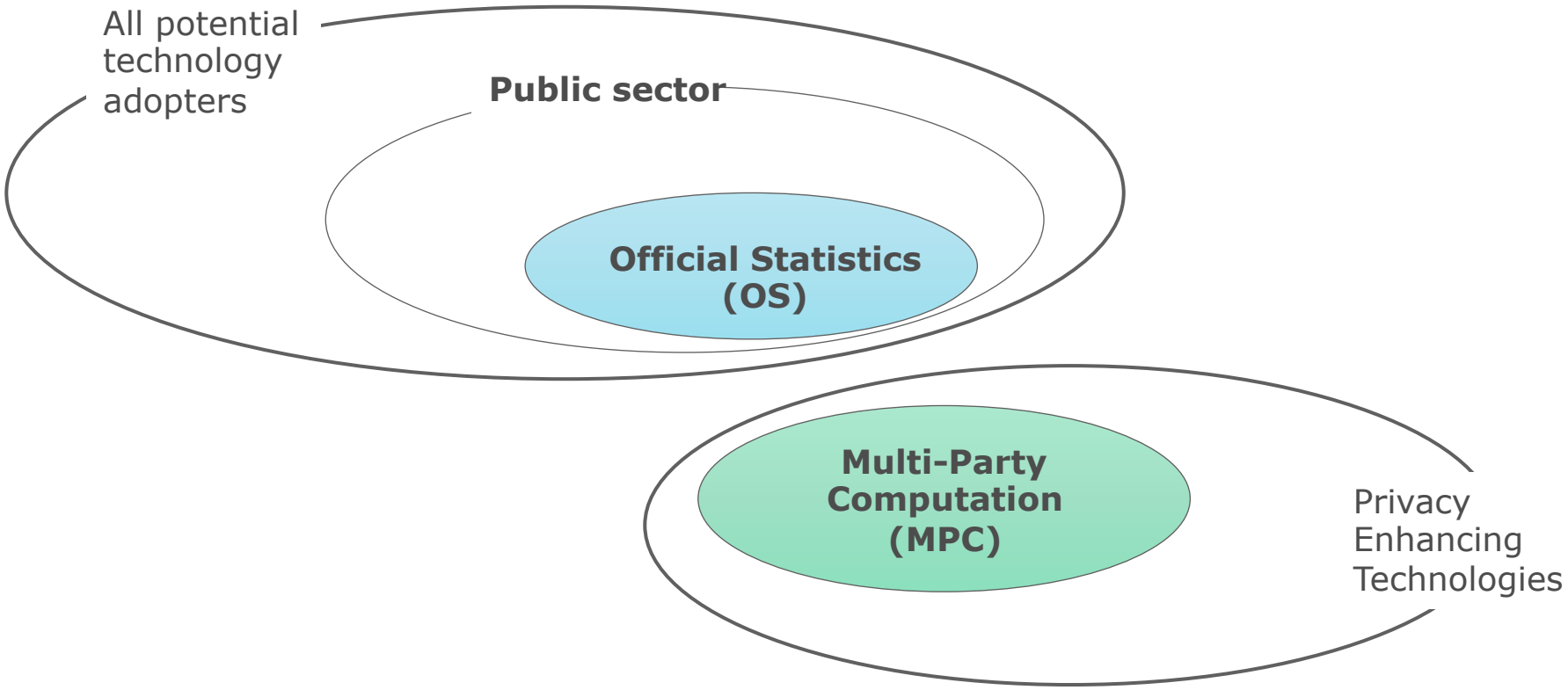
Goal of this talk

Offer a reflection on the potential role of MPC in Official Statistics from the perspective of potential adopters of MPC technologies

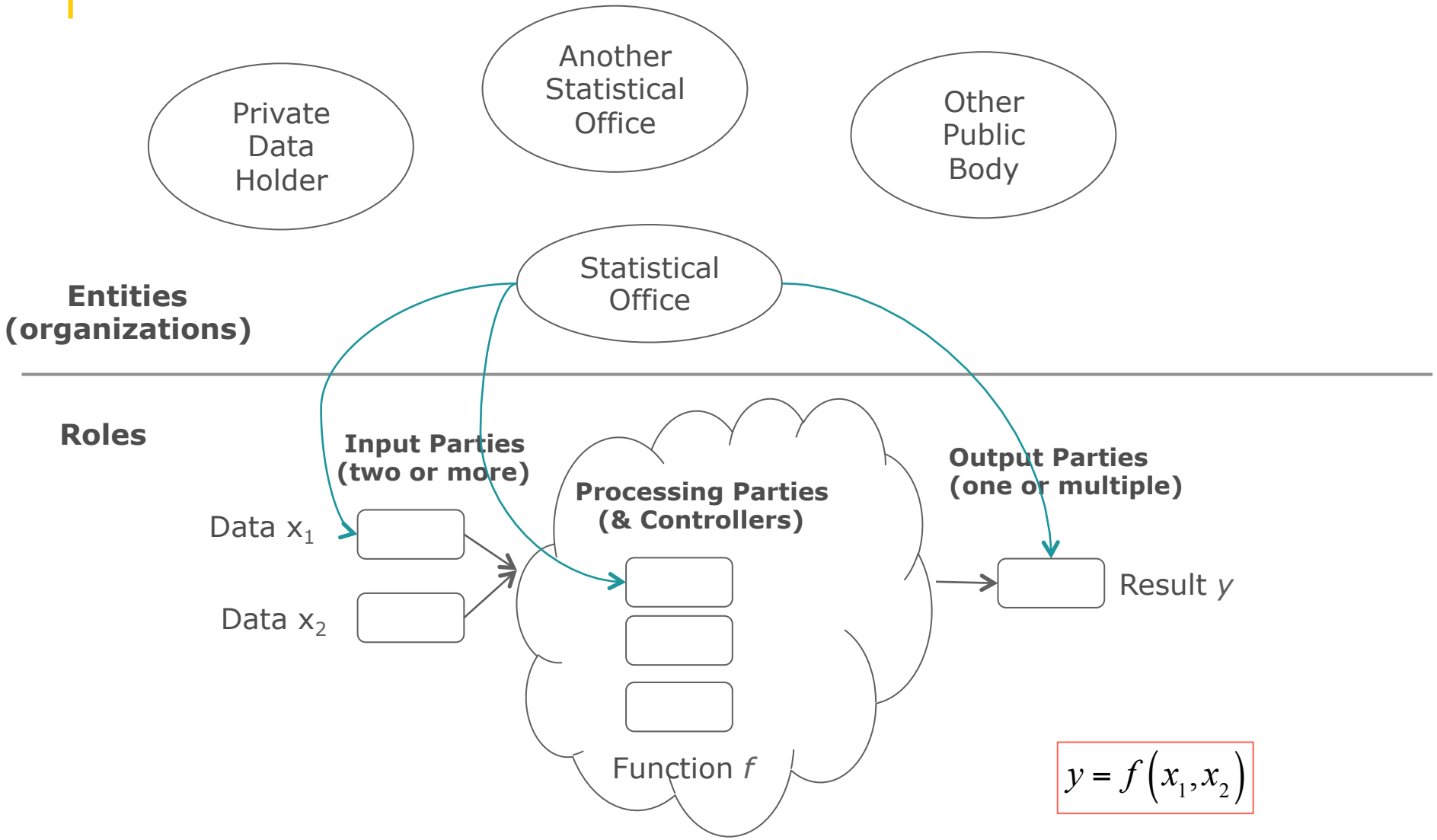
Caveat

The information and views set out in this presentation are those of the author and do not necessarily reflect the official opinion of the European Union. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein.

Scoping this talk



Setting the scene



MPC-for-OS relevant scenarios

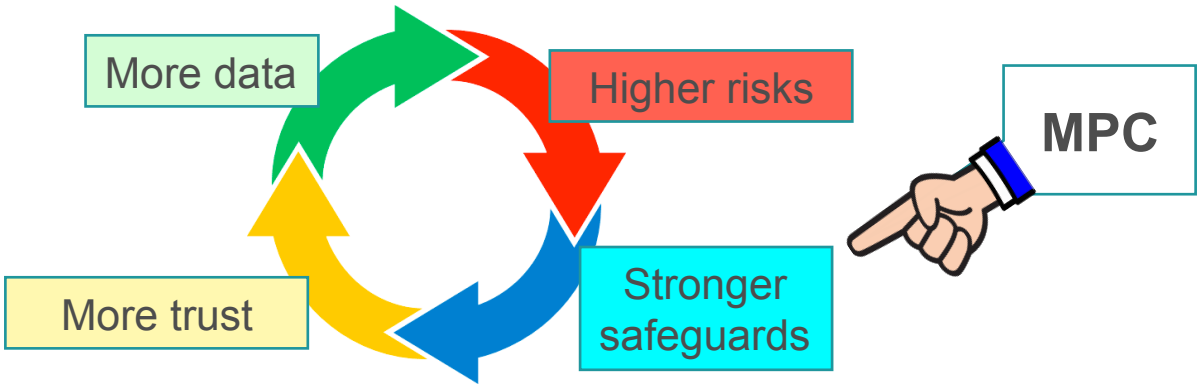
We see a role for MPC in OS when:

- The input data are held by multiple Input Parties (two or more)
  - if all input data are at a single entity, computation may be centralized therein
- At least one statistical office is involved in the role of Input Party and/or Output Party
  - Possibly, but not necessarily, also as processing party
- NB: in OS the function *f* is *not* secret (methodological transparency)
  - Things may be different in the private sector where *f* may be proprietary

OS : Official Statistics
MPC : Multi-Party Computation

Why do we care?

- Increasing appetite for cross-organisational data processing in the context of Official Statistics innovation
  - Data held by national authorities in different countries concerning cross-border phenomena (e.g., int'l trade, migration, …)
  - Statistics based on data held by other public bodies (e.g., administrative data)
  - New statistics based on privately held data requiring integration across different providers (often competitors in the same business sector) and with data held by statistical authorities
- Increasing awareness of the importance of (personal) data protection by the general public



Options

- Do nothing (abstain from computation)
- Exchange input data between the involved entities
- Exchange input data with a Trusted Third Party
- Adopting a Secure MPC solution

All these options are legitimate and may be preferred in different contexts.

Option selection is a matter of minimising jointly the (actual or perceived) **risks** and **costs**. Therefore potential adopters need to understand the risks and costs of MPC-based solutions, compared to the other options.
Key dimensions shaping costs and risks include: legal compliance, trust model …

Legal compliance

- In our current understanding, MPC-based solutions qualify as *processing of personal data* and therefore remain within GDPR
  - MPC solutions as *supplementary "technical and organisational measures"* in the sense of GDPR Art. 89 (*,**)
- Well-designed MPC solutions, based on strong implementations of state-of-the-art technologies, can be effective means of compliance with GDPR
  - Embracing GDPR principles as 'design requirements' for MPC-based solutions: data minimisation, purpose specification, storage limitation …

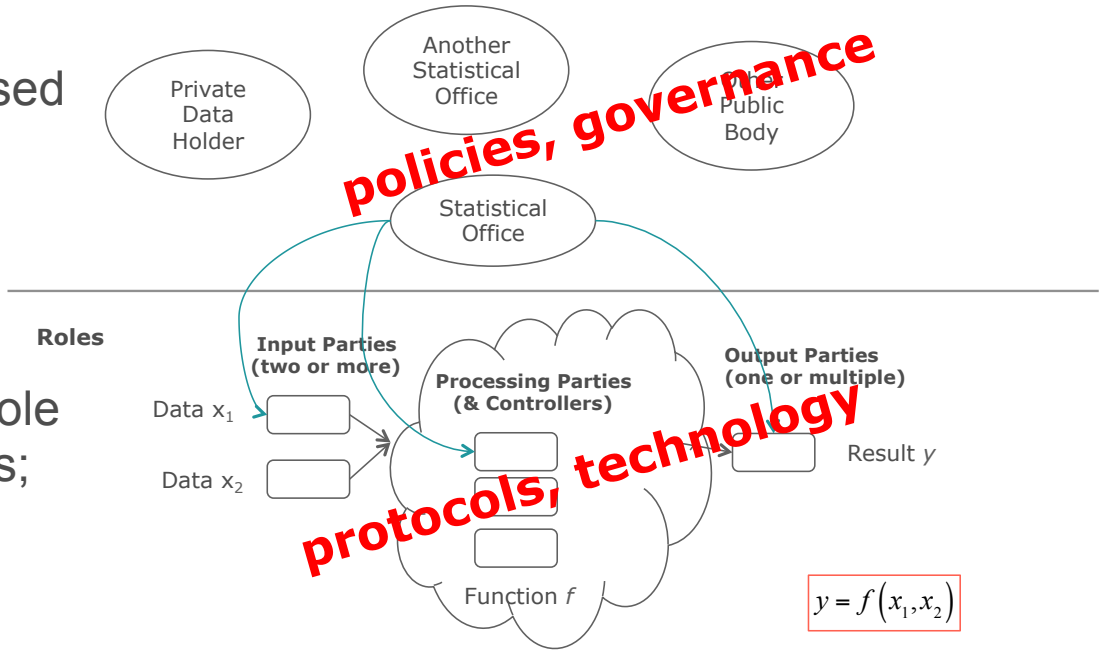
(*) In line with EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Use Case 5: Split or multi-party processing)

(**) In line with ENISA view, see report on "Data Pseudonymisation: Advanced Techniques and Use Cases", January 2021

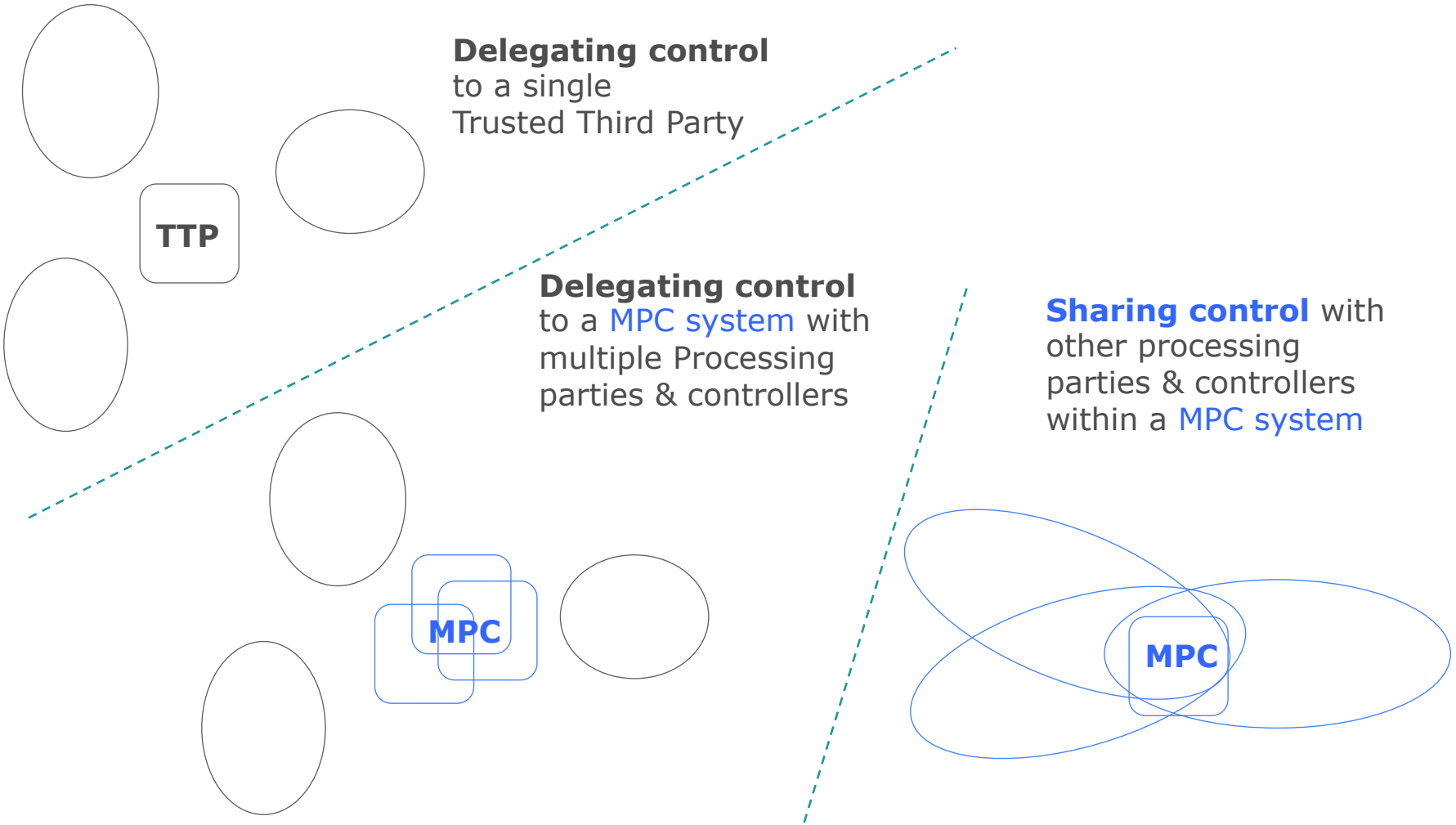
Trust model

- The essential role of MPC is to enforce technologically the governance/policies (for data & code) defined among entities
- Goal: avoid single-point-of-trust (SPoT) → the set of processing parties are to be trusted *collectively, not individually*
- If you don't trust the other processing parties, be a processing party yourself!

- The overall strength of MPC-based solution depends *jointly* on
- (i) robustness of policies/governance scheme;
- (ii) choice of entities taking the role of processig parties & controllers;
- (iii) strength of technology implementation

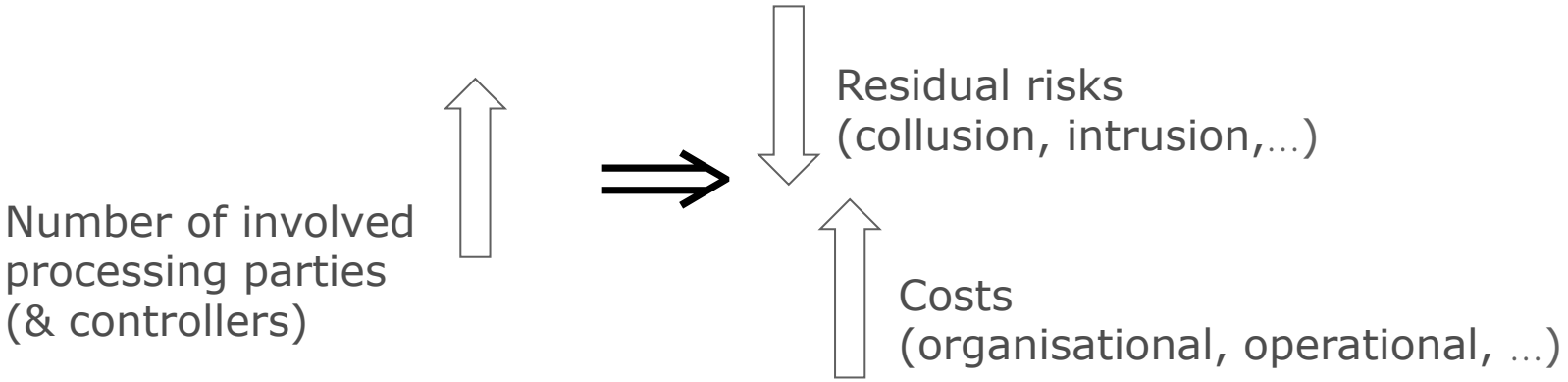


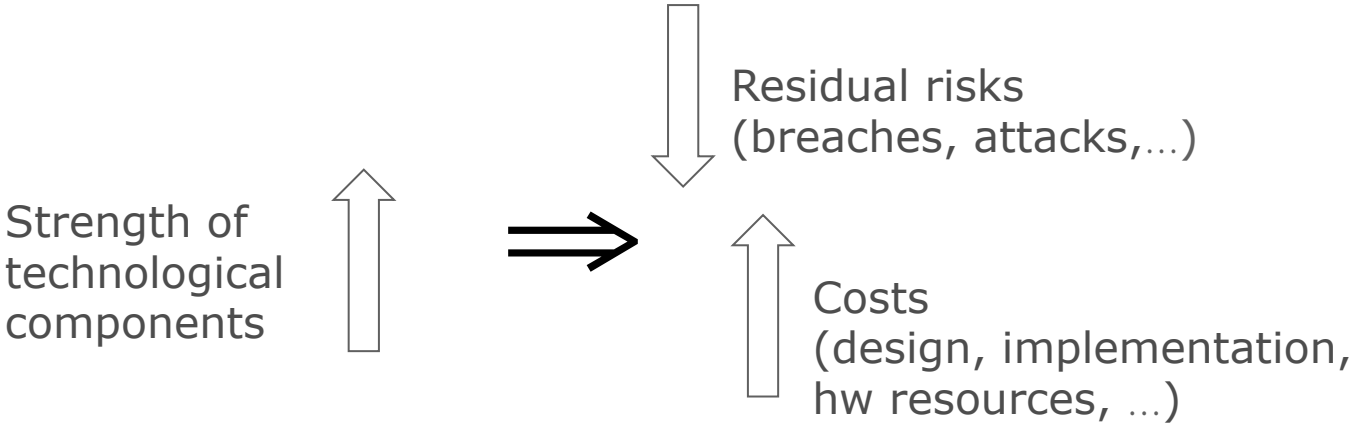
From delegation to sharing (of processing control)



Explanation: ovals represent Input Parties and Output Parties.
Rectangles represent processing parties & controllers

Cost-Risk trade-offs



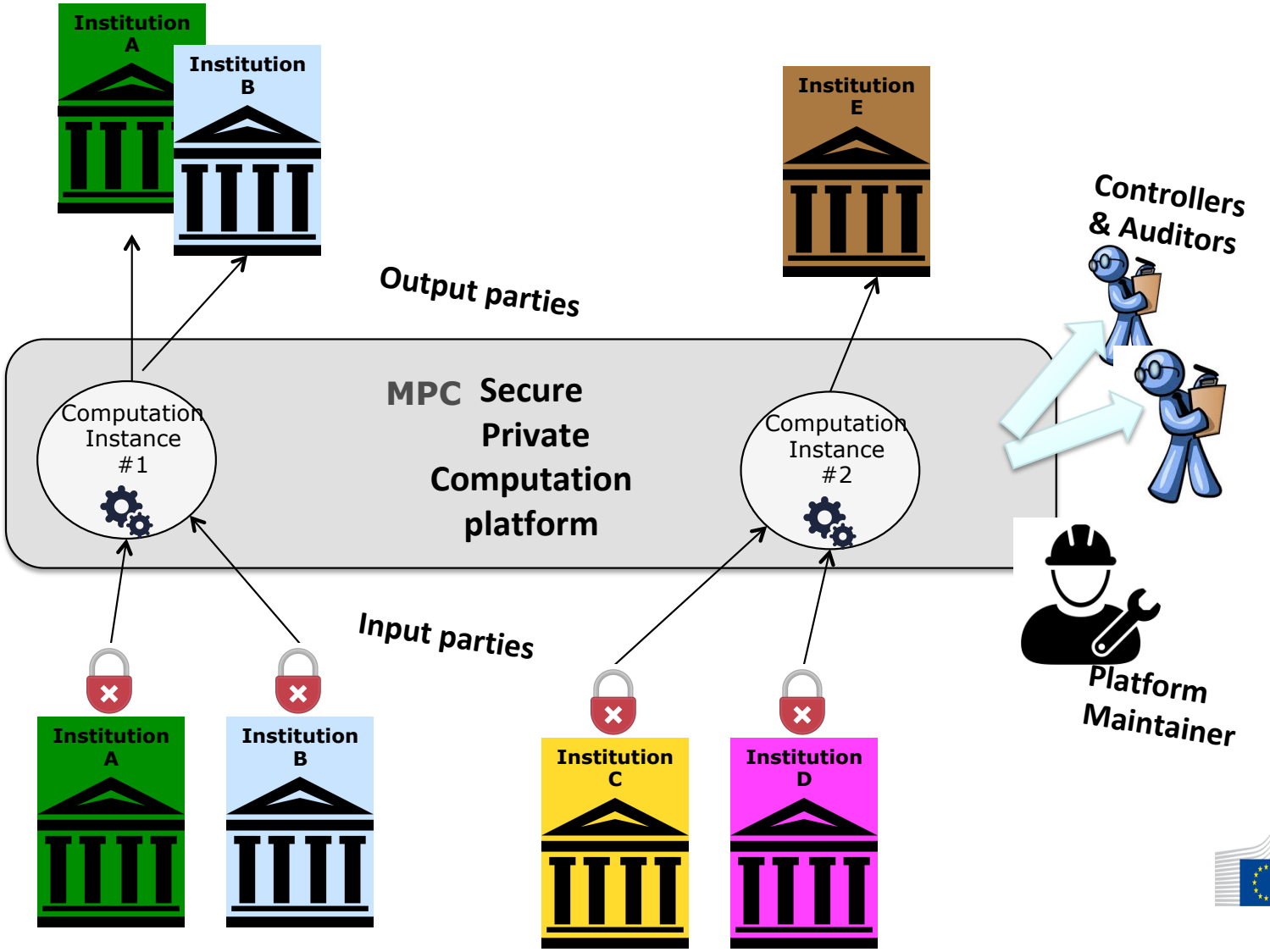


Joining forces among potential adopters

- Q. How to make the strongest possible MPC solution with lowest risk affordable *for the adopters*?

Shared MPC platform → MPC-as-a-service

MPC Secure Private Computing-as-a-service



European Commission

MPC Secure Private Computing-as-a-service

- Built and operated by a consortium/network *of* public institutions *for* public institutions and their private partners
- Team-up with specialised technology providers for co-design of all-round solution (policies & protocols)
- Consultation with Data Protection Authorities already at design phase to ensure legal compliance – *taking GDPR principles as design requirements?*

Take-home message

- MPC-based solutions as alternative to plain data sharing have an important role to play (also) in the future of Official Statistics
- Technology may be already mature, but adoption still slow due to other factors – fundamental paradigm change at stake
- Shared MPC-as-a-service platform as possible way to facilitate adoption in the public sector, and particularly in OS
- Co-design of all-round solutions between technology providers and potential adopters is the way to go.

Thank you for your attention

More about the work done at Eurostat on Privacy Enhancing Technologies for Official Statistics:

https://ec.europa.eu/eurostat/cros/content/privacy-enhancing-technologies-official-statistics-pet4os_en