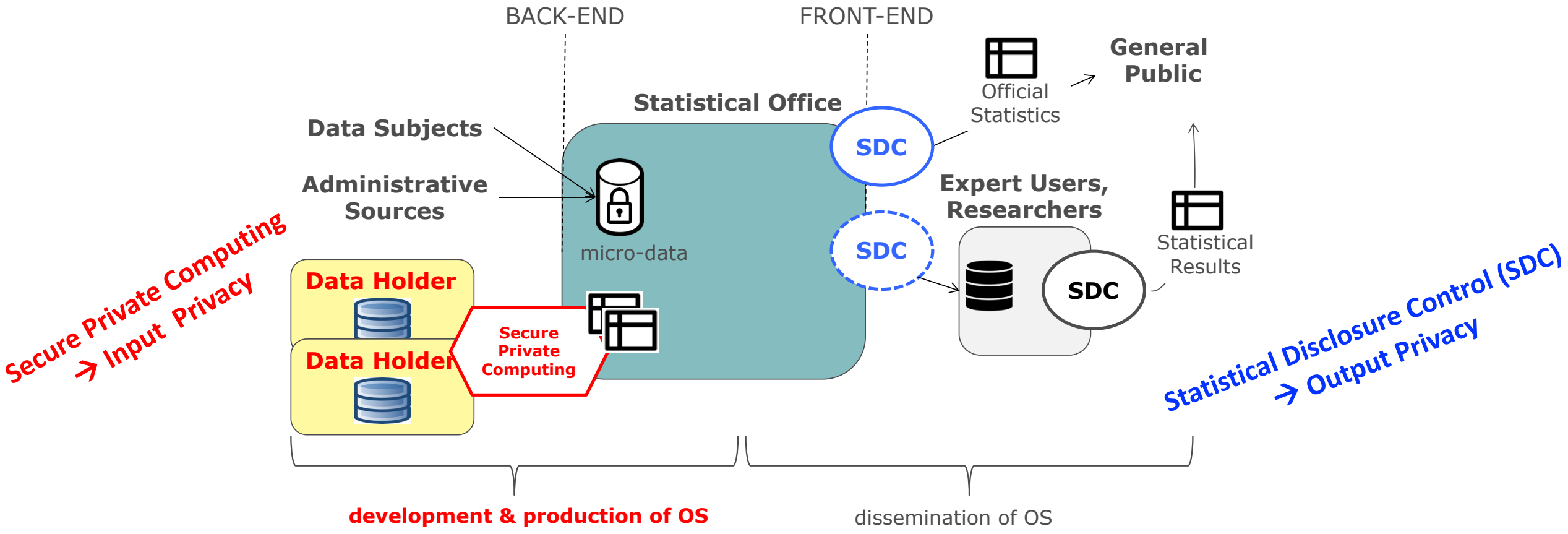
# Track 3 - Open Technical consultation on Multi-Party Secure Private Computing-as-a-Service (MPSPCaaS)

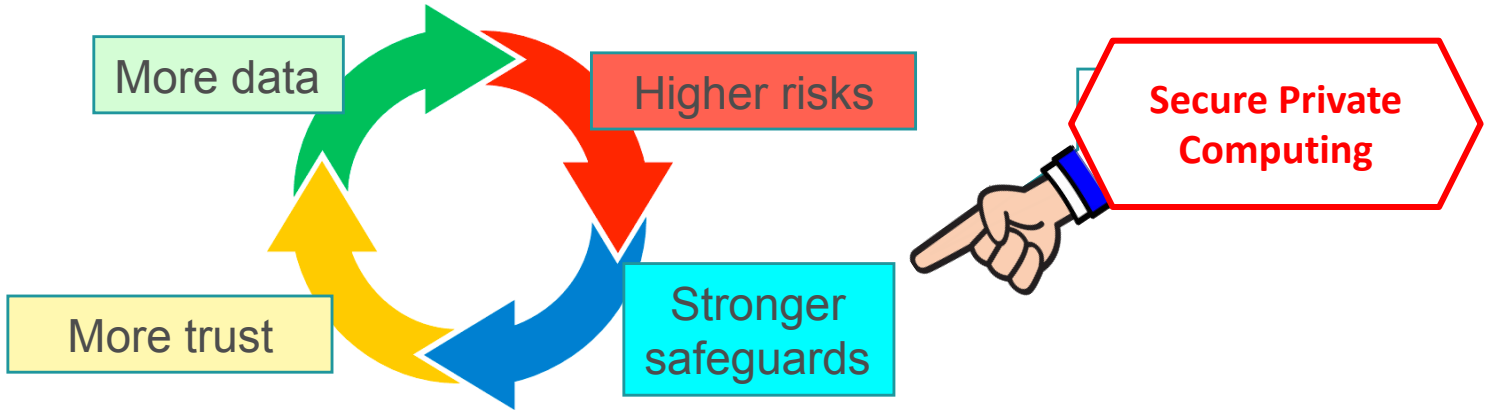
Fabio Ricciato, Eurostat

# Input Privacy and Output Privacy



# Context and trends

- Increasing demands for **cross-organisational data processing** the context of Official Statistics resulting from multiple innovation trends
  - Data held by national **authorities in different countries** to be combined/matched for statistics referred to cross-border phenomena (e.g., int'l trade, migration)
  - Reuse of **data held by other public bodies** for statistics (e.g., administrative registers)
  - New statistics based on **privately held data** requiring integration across different providers (often competing companies) and with data held by statistical authorities
- Increasing **awareness by the public** about the importance of personal data protection



# How to implent **cross-organisational data processing** ?

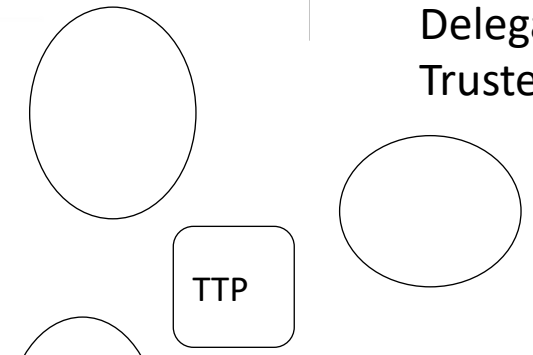
- Don’t implement - abstain from computation
- Exchange input data between the involved entities (traditional data sharing)
- Exchange input data with an external Trusted Third Party
- **Adopting a (Multi-party) Secure Private Computing solution**

Different options may be preferred in different contexts. The choice is a matter of minimising jointly the (actual or perceived) **risks** and **costs**.

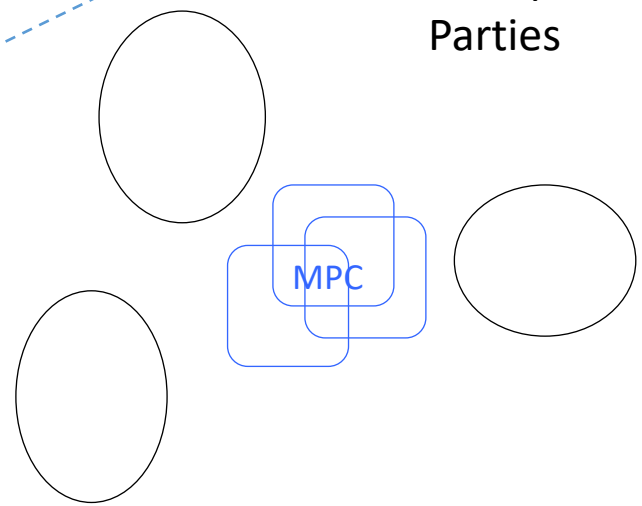
→ Potential adopters need to understand the risks and costs of Secure Private Computing solutions compared to the other options.

# From *delegation* to *sharing* of computation control

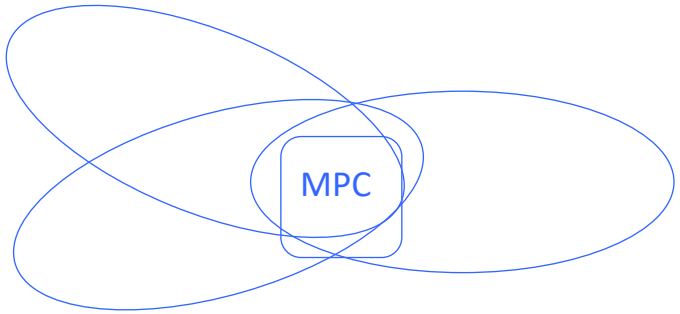
Delegating control to a single Trusted Third Party (TTP)




Delegating control to a MPC system with multiple Processing Parties




Sharing control with other processing parties & controllers within a MPC system




Explanation: ovals = Input Parties & Output Parties; rectangles = Processing Parties
MPC : Multi-Party Computation

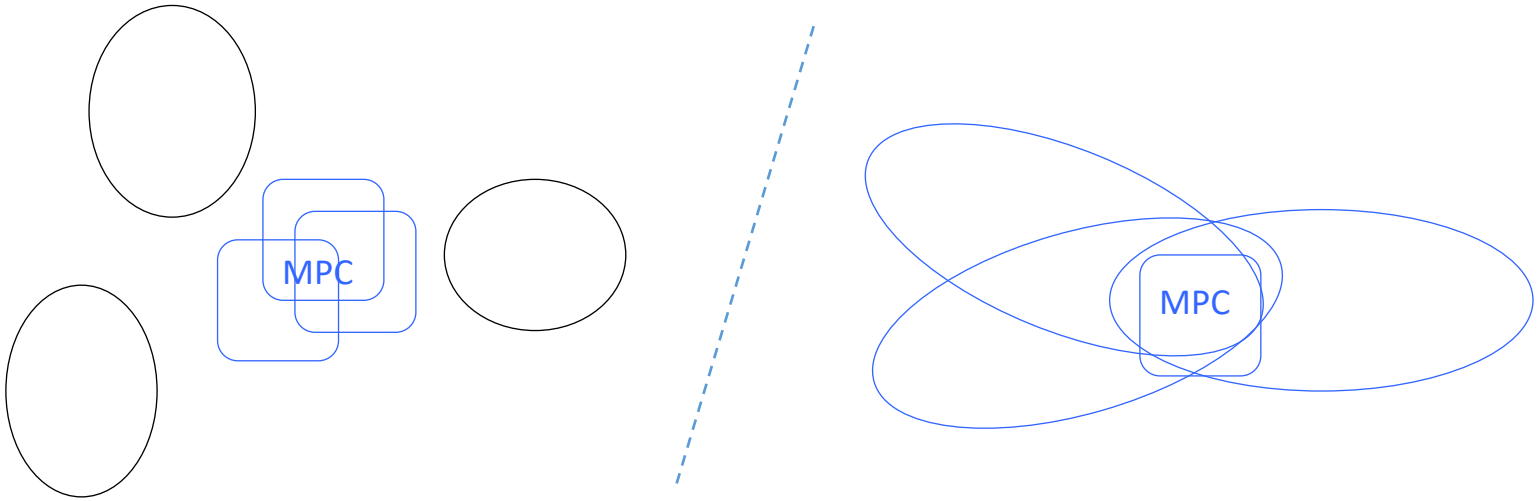
# Cost-Risk trade-offs

Number of processing parties ⇑ ⇒ ⇓ Residual risks (collusion, intrusions,…)

⇑ Costs (organisational, operational, …)

Strength of technological components ⇑ ⇒ ⇓ Residual risks (breaches, attacks,…)

⇑ Costs (implementation, maintenance, HW/SW …)



# MultiParty Secure Private Computing-as-a-Service (MPSPCaaS)

Q. How to make the strongest possible MultiParty (MP) Secure Private Computing (SPC) solution affordable *for the adopters*?

- Lowest possible risk at acceptable cost

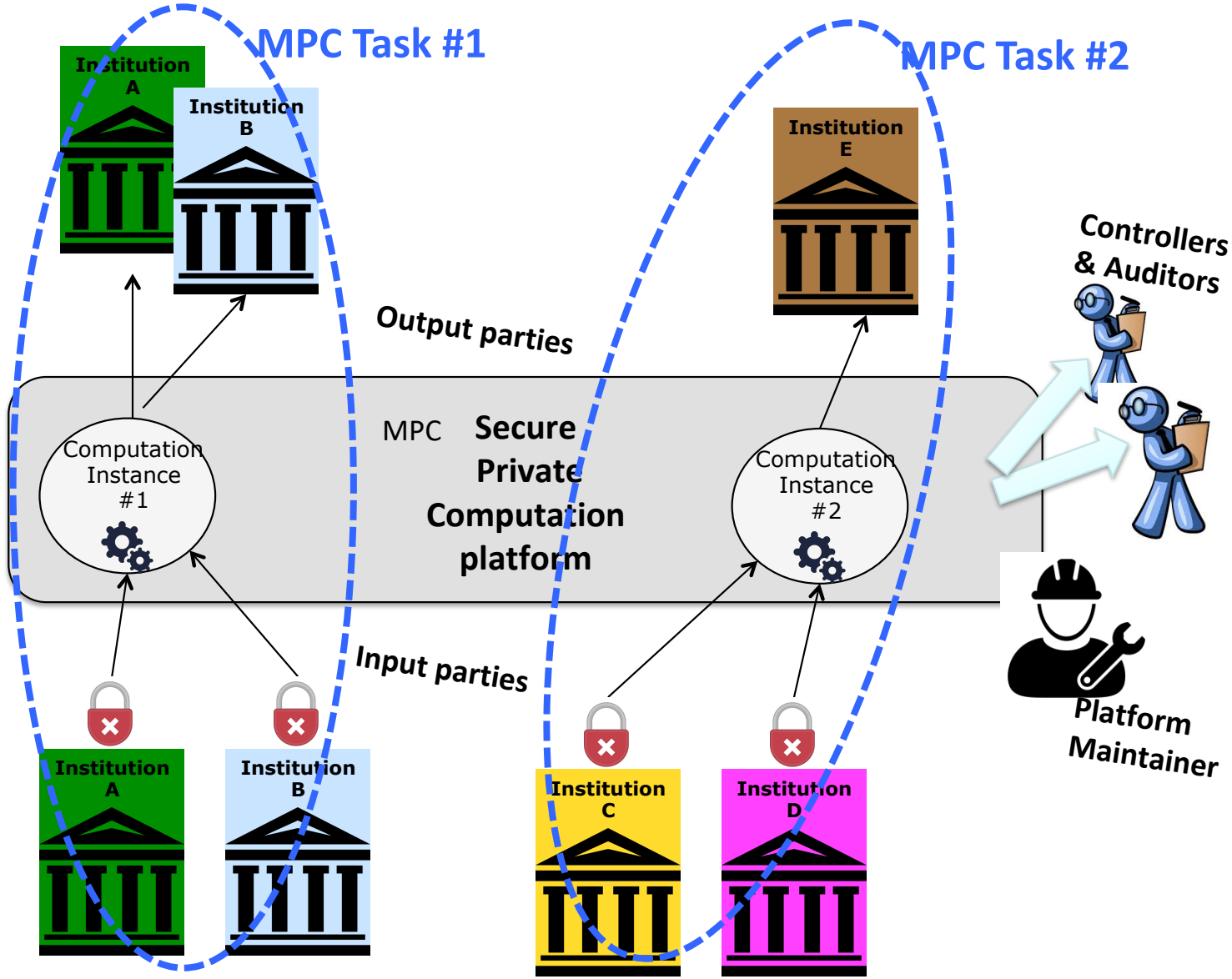
Shared MPSPC platform → MPSPC-as-a-service

# MPSPCaaS

Build once,
use for multiple
computation tasks

Decouple **building**
the MPSPC infrastructure
from **using** it
to perform secure
computation tasks

Turn a technological
**system** into a **service**



# MPSPCaaS concept casted in Official Statistics

MPSPCaaS infrastructure is designed, built and operated by a consortium/network *of* statistical institutions *for* statistical institutions (+ their private partners)

- E.g., European Statistical System (ESS)

Team-up with specialised technology providers for co-design of all-round solution tailored to the needs of statistical offices

- Design jointly technological & organisational components; protocols & policies

Consultation with Data Protection Authorities already at design phase to ensure legal compliance

# SPC and GDPR

- In our current understanding, SPC solutions qualify as *processing of personal data* and therefore remain within the scope of GDPR
  - SPC solutions as *supplementary "technical and organisational measures"* in the sense of GDPR Art. 89 (*,**)

- Well-designed SPC 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 SPC solutions: data minimisation, purpose specification, storage limitation, integrity and confidentiality …

(*) 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)

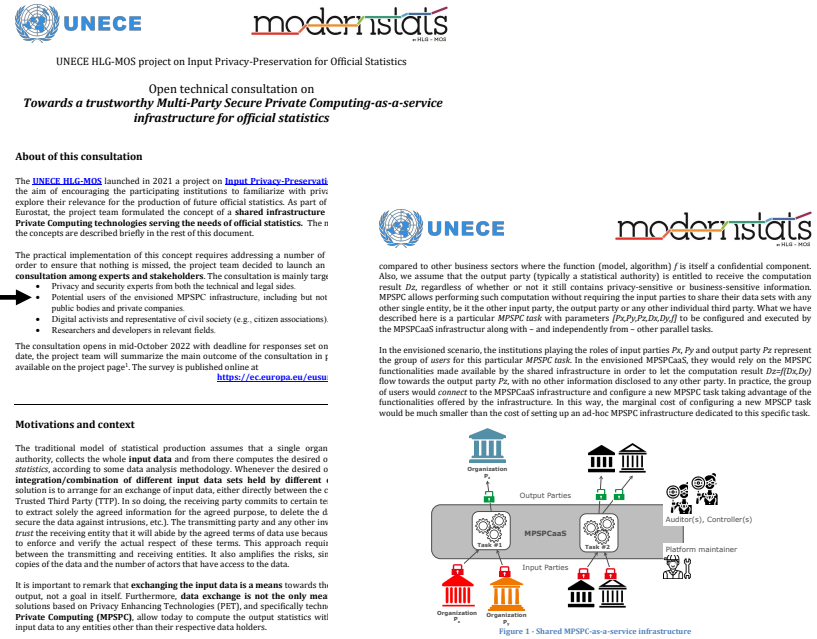
(**) In line with ENISA view, see report on "Data Pseudonymisation: Advanced Techniques and Use Cases", January 2021

# Open Consultation (Track 3 of IPP)

- MPSPCaaS concept formulated within the UNECE HLG-MOS Input Privacy-Preservation project (IPP)
- Innovative -- maybe too innovative?
- Have we considered all aspects, technical and non-technical?
- What do the stakeholders out there think of it?
  - Prospective users? Technology experts? Privacy experts?
- Let's ask them! → Launch a Open Technical Consultation

# Open Technical Consultation

- Short 5-pages document (link) to describe the MPSPCaaS concept
- Online consultation via EUSurvey tool (requires EUlogin account), participation link: https://ec.europa.eu/eusurvey/runner/MPSPCaaS2022
- 8+1 questions, free text replies.
- Consultation open from mid-October to end-November
- Invitations sent to initial list of experts, with request to circulate it further – call for participation online on wiki https://statswiki.unece.org/display/IPP/Input+Privacy-Preservation+for+Official+Statistics+Home
- Follow-up: analysis of responses during December'22; drafting of high-level summary of received feedback and inclusion in the IPP project final report



UNECE HLG-MOS project on Input Privacy-Preservation for Official Statistics

Open technical consultation on

***Towards a trustworthy Multi-Party Secure Private Computing-as-a-service infrastructure for official statistics***

**About of this consultation**

The UNECE HLG-MOS launched in 2021 a project on Input Privacy-Preservati
the aim of encouraging the participating institutions to familiarize with priv
explore their relevance for the production of future official statistics. As part of
Eurostat, the project team formulated the concept of a **shared infrastructure**
**Private Computing technologies serving the needs of official statistics.** The n
the concepts are described briefly in the rest of this document.

The practical implementation of this concept requires addressing a number of
order to ensure that nothing is missed, the project team decided to launch an
**consultation among experts and stakeholders**. The consultation is mainly targ

- Privacy and security experts from both the technical and legal sides.
- Potential users of the envisioned MPSPC infrastructure, including but not public bodies and private companies.
- Digital activists and representative of civil society (e.g., citizen associations).
- Researchers and developers in relevant fields.

The consultation opens in mid-October 2022 with deadline for responses set on
date, the project team will summarize the main outcome of the consultation in
available on the project page[1]. The survey is published online at
https://ec.europa.eu/eusu

**Motivations and context**

The traditional model of statistical production assumes that a single organ
authority, collects the whole **input data** and from there computes the desired o
*statistics*, according to some data analysis methodology. Whenever the desired o
**integration/combination of different input data sets held by different**
solution is to arrange for an exchange of input data, either directly between the
Trusted Third Party (TTP). In so doing, the receiving party commits to certain te
to extract solely the agreed information for the agreed purpose, to delete the d
secure the data against intrusions, etc.). The transmitting party and any other inv
*trust* the receiving entity that it will abide by the agreed terms of data use becaus
to enforce and verify the actual respect of these terms. This approach requi
between the transmitting and receiving entities. It also amplifies the risks, sin
copies of the data and the number of actors that have access to the data.

It is important to remark that **exchanging the input data is a means** towards th
output, not a goal in itself. Furthermore, **data exchange is not the only mea**
solutions based on Privacy Enhancing Technologies (PET), and specifically techn
**Private Computing (MPSPC)**, allow today to compute the output statistics wit
input data to any entities other than their respective data holders.

[1] Webpage of the project: https://statswiki.unece.org/display/IPP/Input+Privacy-Preserv

UNECE modernstats

compared to other business sectors where the function (model, algorithm) *f* is itself a confidential component. Also, we assume that the output party (typically a statistical authority) is entitled to receive the computation result *Dz*, regardless of whether or not it still contains privacy-sensitive or business-sensitive information. MPSPC allows performing such computation without requiring the input parties to share their data sets with any other single entity, be it the other input party, the output party or any other individual third party. What we have described here is a particular *MPSPC task* with parameters *[Px,Py,Pz,Dx,Dy,f]* to be configured and executed by the MPSPCaaS infrastructure along with – and independently from – other parallel tasks.

In the envisioned scenario, the institutions playing the roles of input parties *Px, Py* and output party *Pz* represent the group of *users* for this particular *MPSPC task*. In the envisioned MPSPCaaS, they would rely on the MPSPC functionalities made available by the shared infrastructure in order to let the computation result *Dz=f(Dx,Dy)* flow towards the output party *Pz*, with no other information disclosed to any other party. In practice, the group of users would *connect* to the MPSPCaaS infrastructure and configure a new MPSPC task taking advantage of the functionalities offered by the infrastructure. In this way, the marginal cost of configuring a new MPSCP task would be much smaller than the cost of setting up an ad-hoc MPSPC infrastructure dedicated to this specific task.




Figure 1 - Shared MPSPC-as-a-service infrastructure

**Multi-party = no single point of trust**

At an abstract level, the MPSPC infrastructure intermediating between the input and output parties may be seen as replacing a centralized Trusted Third Party (TTP), as shown in Figure 1. Indeed, if operation of the infrastructure would be such that a single entity would be *technically* able to control the whole computation process, the central controller would represent the *single point of trust* corresponding *de facto* to a TTP. In other words, a Secure Private Computing solution with centralized control would not be fundamentally different from the traditional model of data sharing with a TTP. In order to avoid that, at the heart of the MPSPC paradigm lays the requirement that no single entity should ever be technically capable to take over control of the process. Therefore, MPSPC operation must be designed so as to **avoid any single point of trust**. That means process control must be split (or divided) among a multiplicity of K>1 parties, which will be referred hereafter as *processing parties*[5]. In principle, K=2 processing parties would suffice to meet this formal requirement, but for increased robustness we will assume hereafter a minimum number of processing parties equal to K=3 or higher. Furthermore, in addition to the K processing parties with *active* control over the processing operation, additional entities may be foreseen to act as *passive controllers*, in order to increase the overall level of security and trust.

[5] The abstract notion of *processing party* introduced here may possibly, but not necessarily correspond to the role of *computing parties* in secret sharing schemes. In fact, secret sharing is one among several possible schemes of choice for MPSPC operation. In multi-key encryption schemes, where the equivalent of a single decryption key is split among multiple key holders, the notion of processing party may correspond to key holders.

# 8+1 questions

1. **General feedback**. What do you think about the envisioned concept of a shared MPSPCaaS infrastructure operated *by* and *for* statistical offices? What are the main points of strength and the main points of concern? Write down your thoughts and comments.

2. **Use-cases**. The initial design of (a first version of) the envisioned MPSPCaaS infrastructure would likely focus on supporting a **set of selected use-cases**. Could you provide examples of the kind of use-cases that you consider important in the field of official statistics and you would recommend to be considered as test cases?

3. **Requirements and design criteria**. What should be in your opinion the main technical requirements and design criteria of the envisioned MPSPCaaS infrastructure in order to provide the strongest possible security and privacy guarantees?

4. **Technologies**. What kinds of technologies, or combinations thereof, you would consider as the most suitable building blocks for the envisioned MPSPCaaS infrastructure?

5. **Processing Parties and Controllers.** What criteria should drive the identification of Processing Parties and Controllers in order to maximize trustworthiness of the envisioned MPSPCaaS infrastructure? As for the Fixed-PP model, which organizations in your opinion are best qualified to serve as Processing Parties? And which one(s) as Controller(s)? How they can be incentivised to participate?

6. **Governance**. Beyond the technical privacy and security guarantees, are there additional governance processes required to ensure the safe and trustworthy operation of all parties involved in the MPSPCaaS operation?

7. **Testing and validation**. How should the system be tested to for its performance, accuracy, robustness of its security and privacy and guarantees? How such guarantees should be verified?

8. **Public trust and acceptance.** Assuming that a robust MPSPCaaS infrastructure has been built and deployed, what additional actions should be taken in order to build public trust and acceptance into the proposed model?

9. **Free suggestions.** You are invited to provide below any specific suggestion or comment that does not fall in any of the previous items (free text).

Link to full document

# Thanks for your attention.

For follow-up visit https://statswiki.unece.org/display/IPP/Input+Privacy-Preservation+for+Official+Statistics+Home

or send an email to Fabio.Ricciato <at> ec.europa.eu

… and consider participating to the consultation!