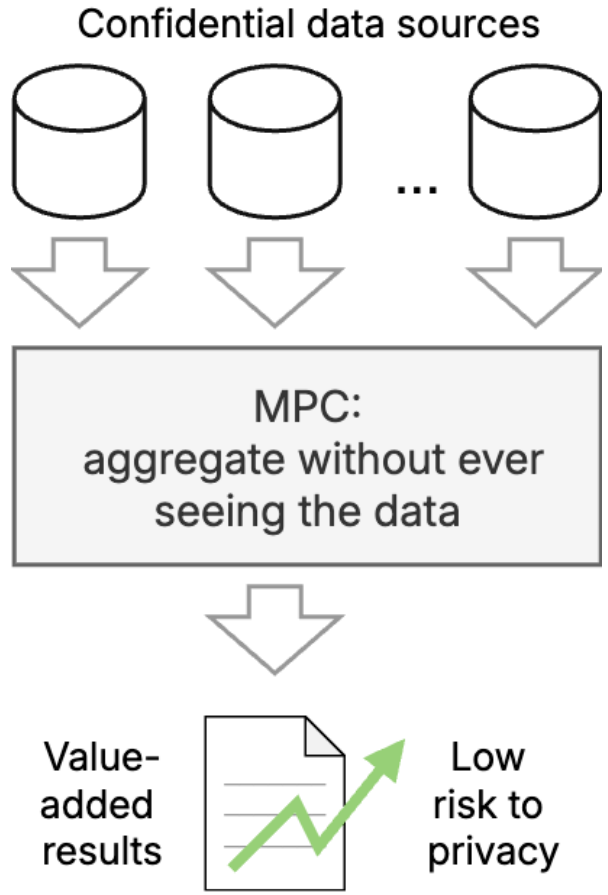
MPC-as-a-service system for official statistics

Riivo Talviste, *PhD*. Sharemind MPC product owner

CYBERNETICA

Problem statement

- Official statistics is changing
  - Privately held data sources (e.g., MNOs)
  - Cross-border collaboration
- Single centralised trusted data aggregator is not viable or not accepted by all parties
- Secure computing is one possible option, specifically MPC



“Don’t lose it, reuse it!”

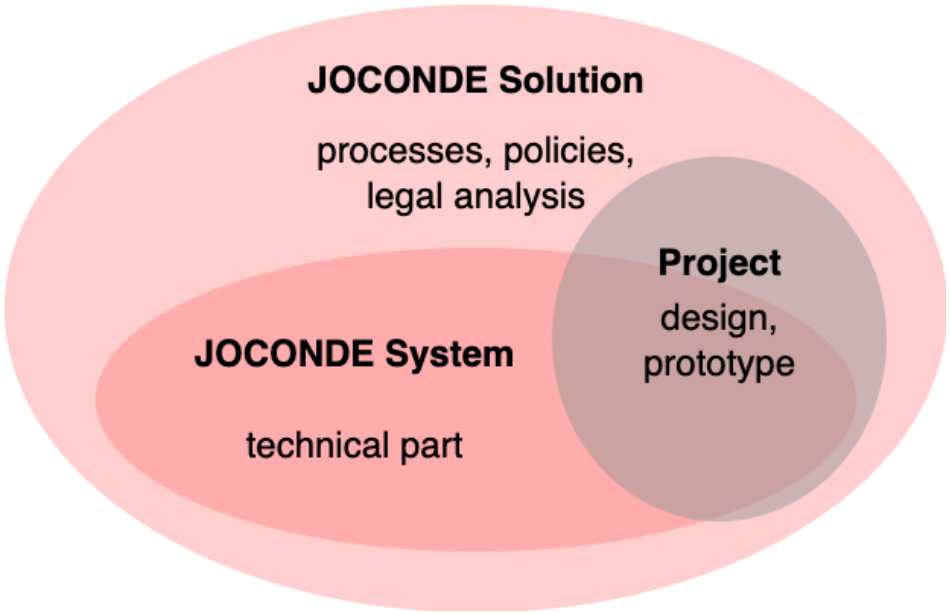
- MPC for data analysis has been done, but
  - It’s a difficult technology to deploy
  - Requires a specific skillset
- Starting from scratch for every pilot is wasteful
- MPC-as-a-service solution reduces complexity
- JOCONDE is MPCaaS for official statistics in European Statistical System (ESS)
  - A single deployment amortises cost

Image by Google Gemini

CYBERNETICA

The JOCONDE Solution

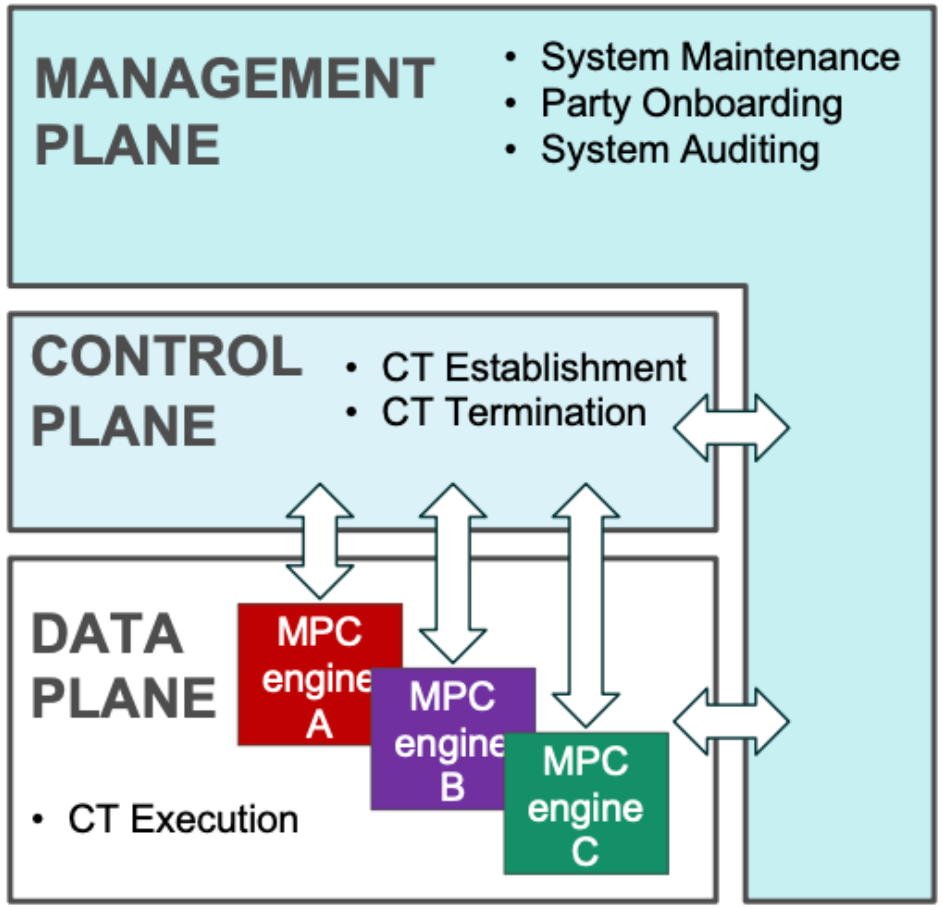
- JOCONDE: Joint On-demand COmputation with No Data Exchange
  - Carried out by Eurostat in collaboration with Cybernetica



- Tasks in the JOCONDE Project:
  1. **Usage scenarios and system requirements**
  2. Technology analysis
  3. Legal aspects
  4. **System specifications and architecture**
  5. Demonstrator prototype and functional testing
  6. Trust building plan

The JOCONDE System (1)

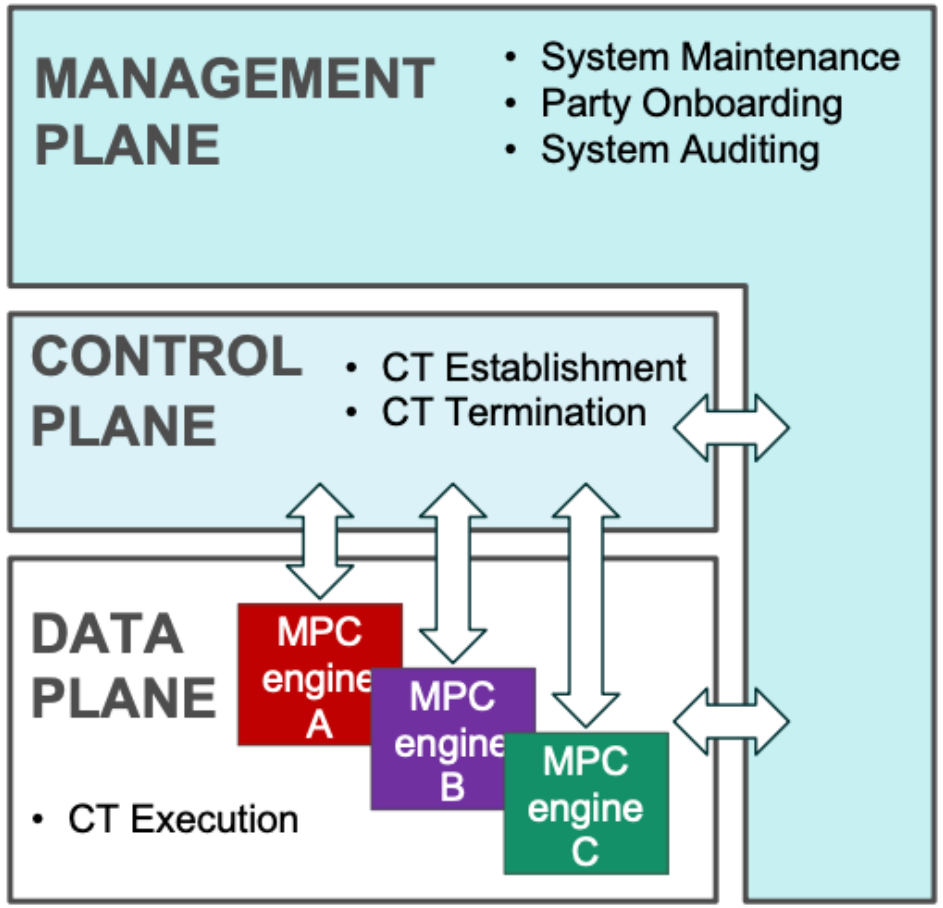
- Management Plane
  - Eurostat is the System Operator (SO)
  - SO manages Members and their identities:
    - Input Parties (IP)
    - Output Parties (OP)
    - Computing Parties (CP)
  - Monitoring and auditing (System Auditor)



CT – computation task
Image source: Fabio Ricciato/Eurostat

The JOCONDE System (2)

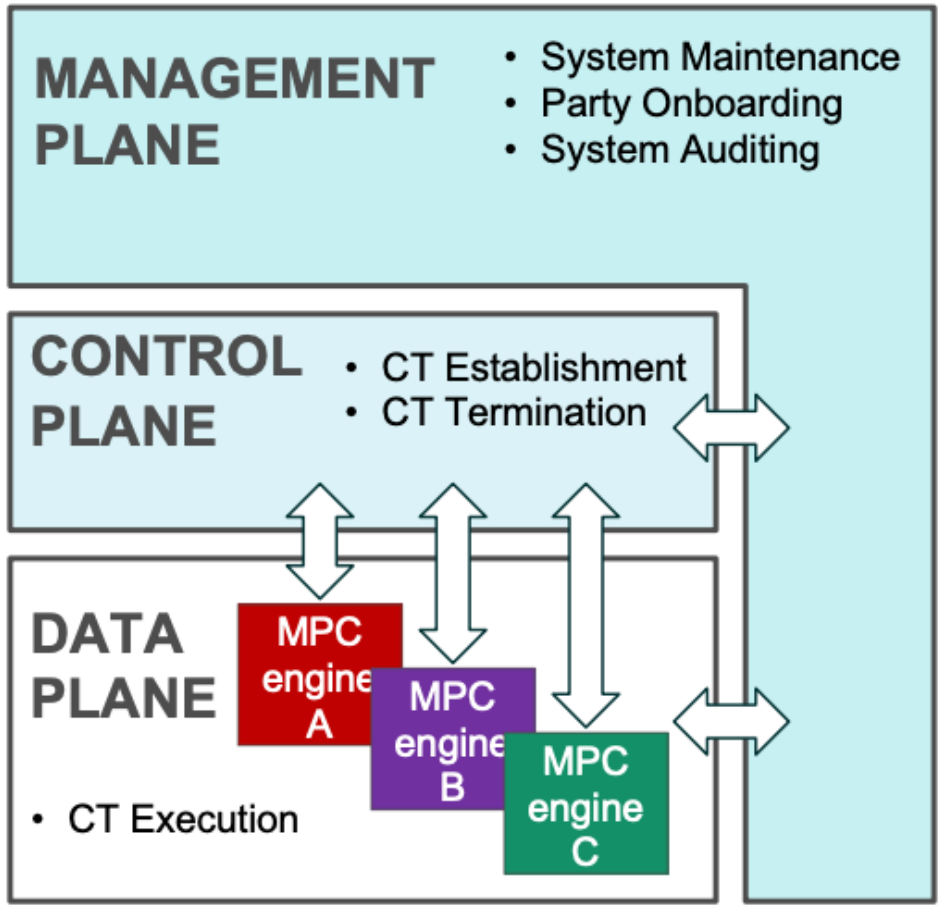
- Control Plane
  - Managing **Computation Task (CT)** lifecycle
  - CT Consortium drafts and signs a CT Specification (CTS) - everything is agreed and set in stone
  - Signed CTS is sent to CPs



CT – computation task
Image source: Fabio Ricciato/Eurostat

The JOCONDE System (3)

- Data Plane
  - Secret sharing and MPC protocols live here
  - List of MPC Engines to choose from (set in CTS)
    - Multiple vendors expected to provide their implementations
  - MPC is run inside Trusted Execution Environment (TEE)
    - Additional layer of confidentiality and integrity



CT – computation task
Image source: Fabio Ricciato/Eurostat

Highlights

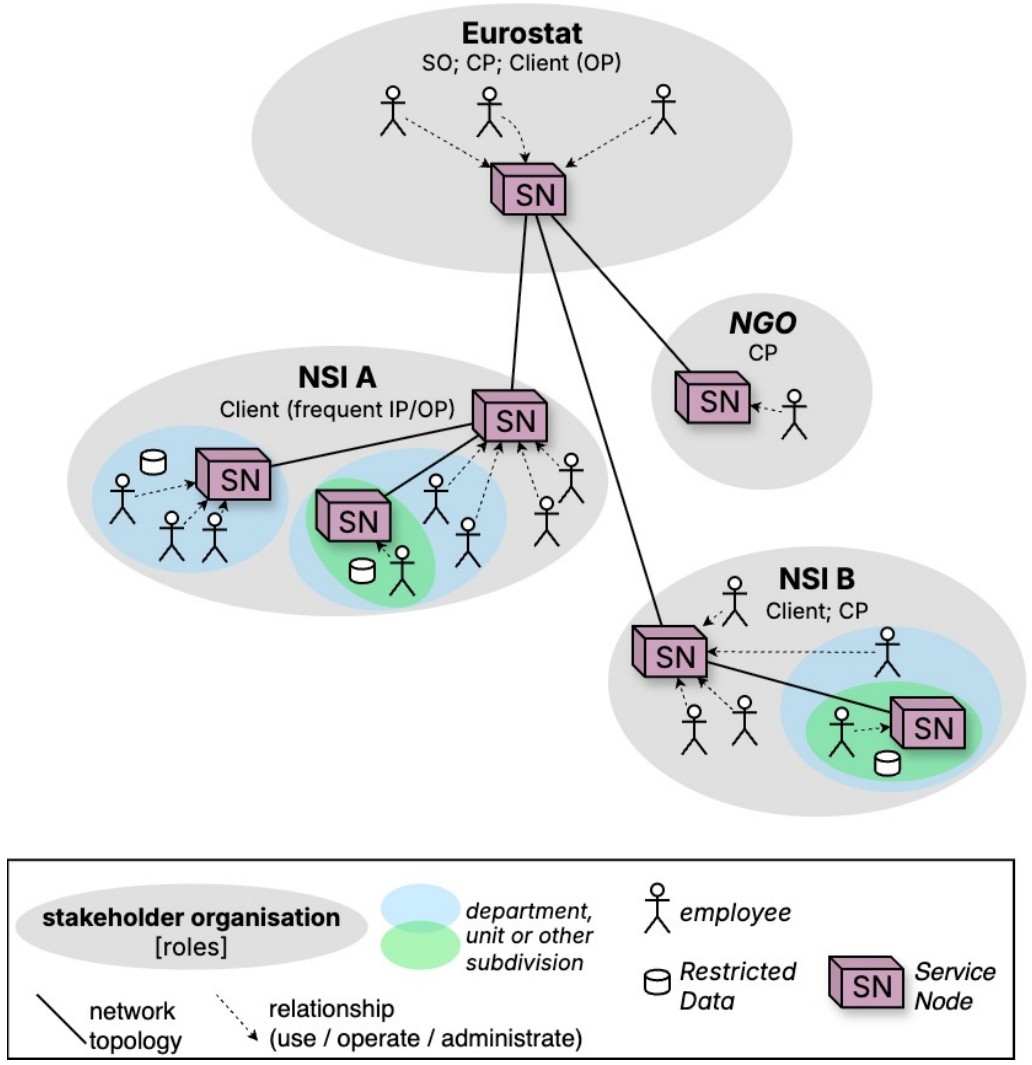
To prevent a “glorified” trusted third party model

Computation Task Specification (CTS)

- Machine readable document = data usage policy enforced by CPs
- Contains:
  - List of Input and Output Parties
    - advisable to verify their public keys out-of-band
  - Data models for input and output data
  - Algorithm to be computed under MPC
    - in high-level open source language
  - List of CPs (out of a set of onboarded nodes)
  - MPC Engine (active/passive, dis/honest majority)
  - Deadlines for providing input, computation, output retrieval
  - Input Data quality algorithms under MPC
    - to prove no malicious intent

Distributed Control Plane

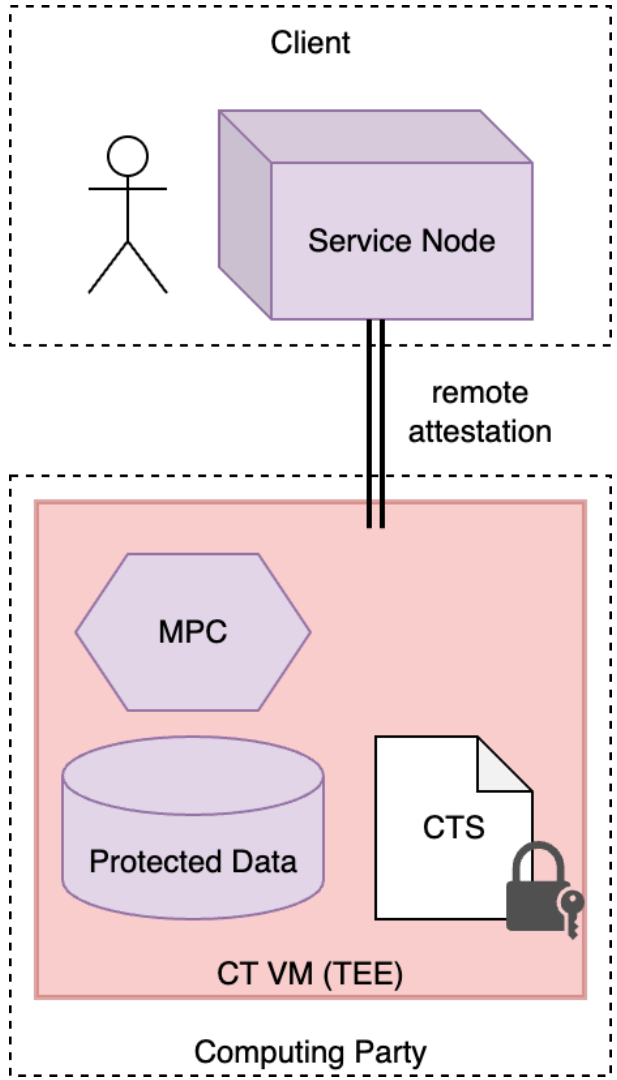
- Each System Member has their own Service Node
- Ad-hoc PKI:
  - SO is root CA and manages System access
  - Each Client (IP/OP) is intermediary CA
  - Internal roles are under Client's control



CYBERNETICA

Data Plane

- Client Node (=Client's Service Node) is trusted
  - Possible to do security critical operations via local web UI
    - secret sharing and data upload
    - sign CTS in the web browser
  - No need for specialised client applications
- Remote code verified using TEE remote attestation
  - MPC Computing Nodes verify each other
  - Clients know that they are talking to actual MPC code
- Restricted Data retention is kept minimal
  - Also no backups of Restricted Data



CYBERNETICA

Host a Computing Node

- CT Consortium Member may take the role of a Computing Party
  - Possibility to halt Computation Task execution
- Combined with actively secure MPC with dishonest majority, gives the strongest control over one's data

Image by Google Gemini

Thank you!

Published project deliverables:
https://cros.ec.europa.eu/joconde

Implementors, start your (MPC) Engines!

Riivo Talviste
<riivo.talviste@cyber.ee>

https://cyber.ee/
info@cyber.ee
cybernetica
CyberneticaAS
cybernetica_ee
Cybernetica