



Signs of life for secure multi-party computation in protecting data

www.mpcalliance.org

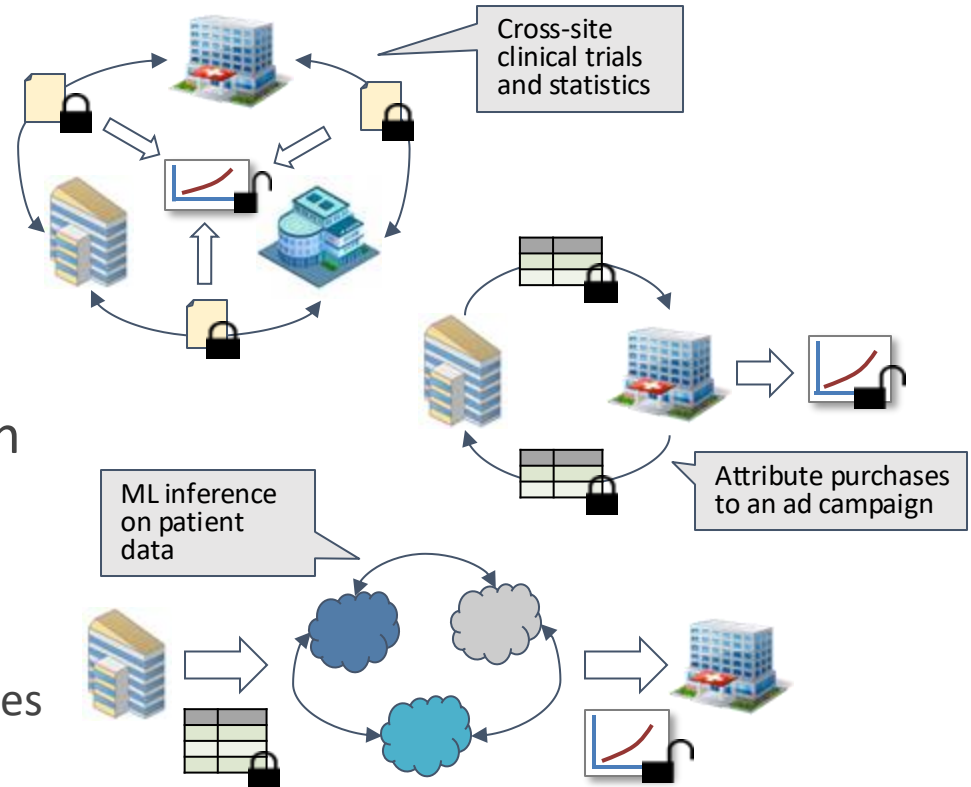
Dr Dan Bogdanov, Member of the Board at MPC Alliance
Chief Scientific Officer at Cybernetica

NIST Workshop on Privacy-Enhancing Cryptography 2024
September 26th, 2024

- **Secure Multi-Party Computation (MPC) for privacy**
- **MPC Alliance Members and Areas of Focus**
- **What is happening in MPC for privacy?**

Secure Multi-Party Computation (MPC) for privacy

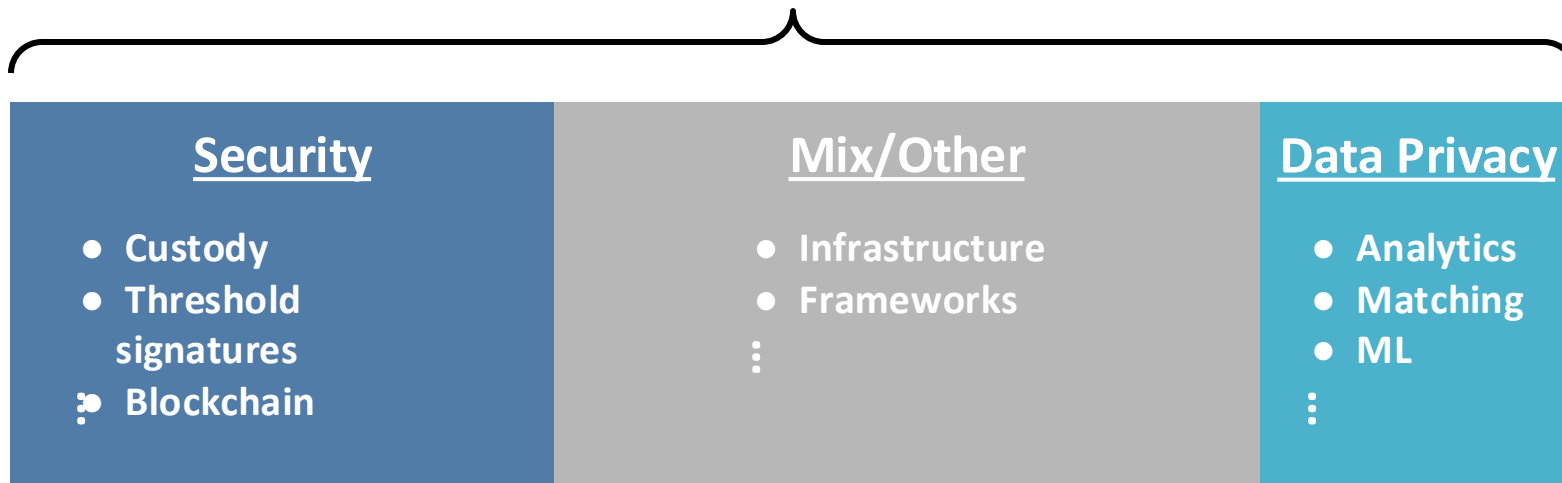
- Two or more parties
 - Multi-party
 - Two-party
 - Outsourced
- *Input* privacy for any function
 - Various security models
- *Output* privacy for any function
 - With differential privacy or
 - Statistical disclosure control
- Decentralised governance
 - Machine-enforced privacy policies



MPC Alliance: Members and Areas of Focus



50+ members

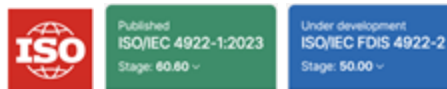


MPC Alliance: Events and Activities

- Event organization and support/participation



- Member organization contributions to standards efforts



- Support/feedback for guidance materials and legislation

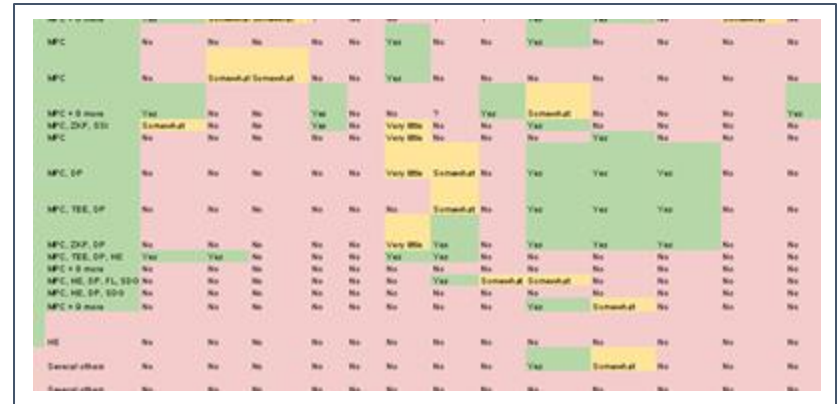


MPCA conducted a privacy enhancing technology report survey

- 28 documents studied, found low coverage of cost, legal aspects and use case aspects

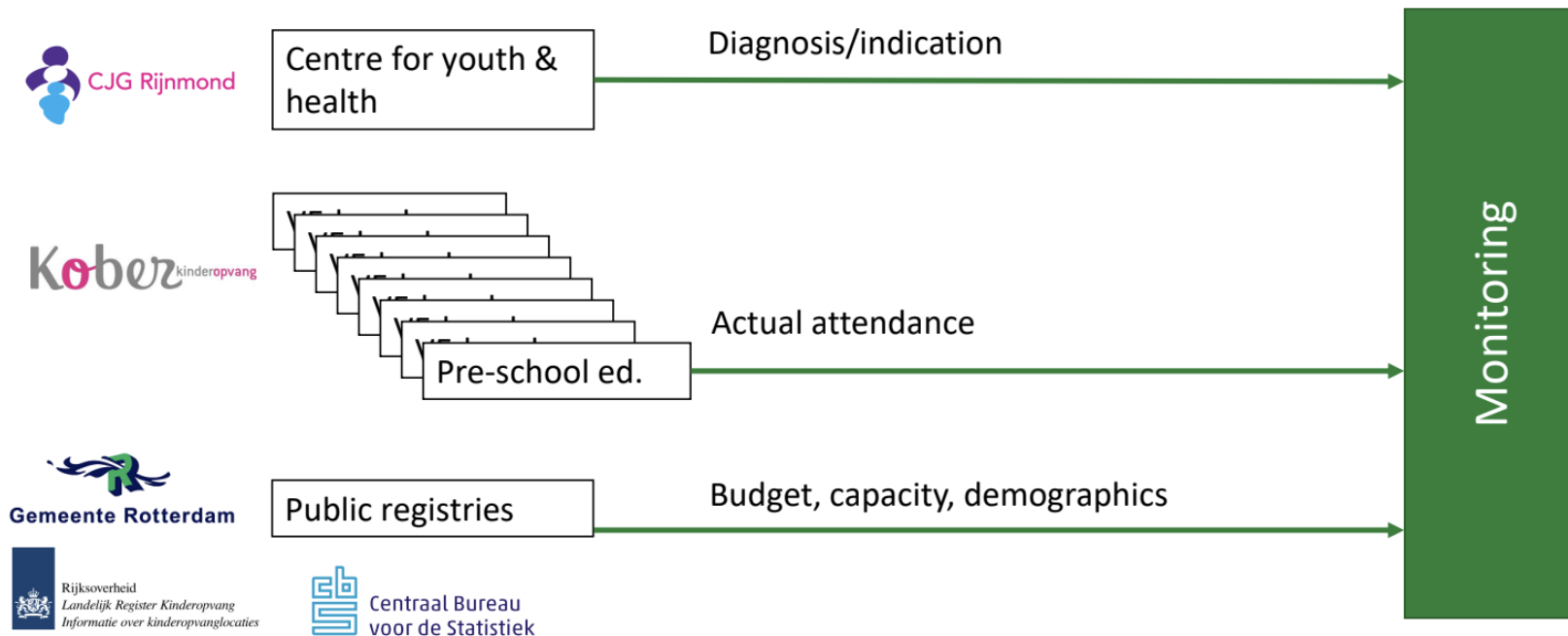
MPCA is working on two reports

1. Blueprints of MPC technology use
2. Value chains of MPC technology



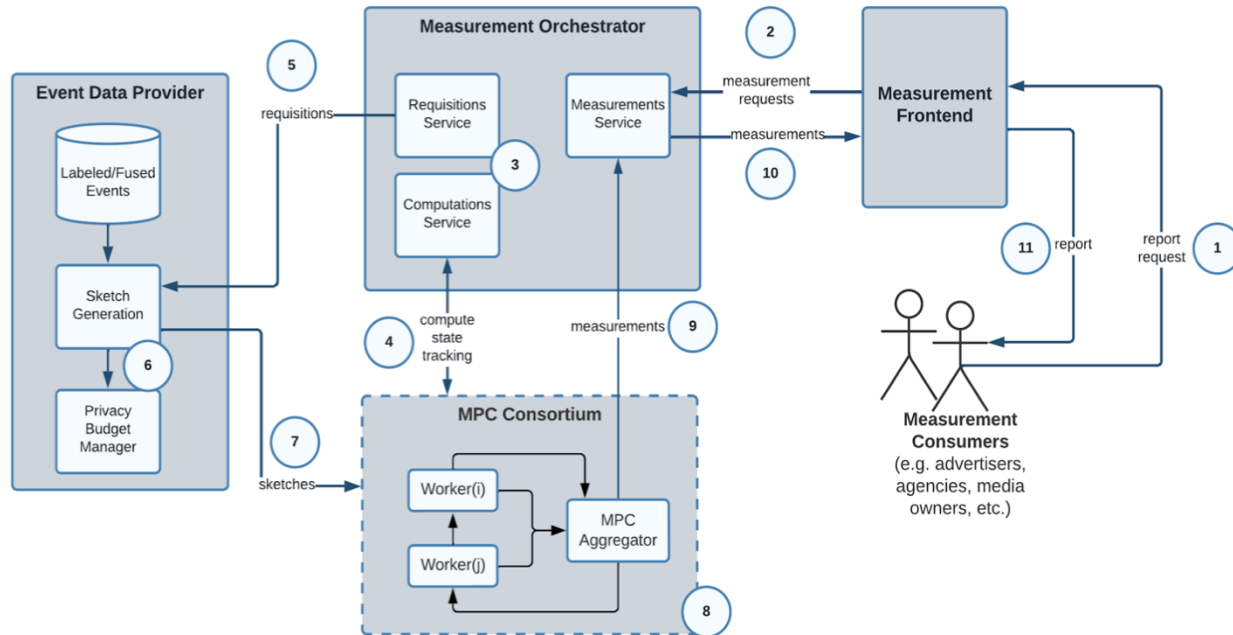
MPC	No	No	No	No	No	Yes	No	No	Yes	No	No	No	No	No
MPC	No	Somewhat	Somewhat	No	No	Yes	No	No	No	No	No	No	No	No
MPC + 9 more	Yes	No	No	Yes	No	No	?	Yes	Somewhat	No	No	No	No	Yes
MPC, DP, SI	Somewhat	No	No	Yes	No	Very little	No	No	Yes	No	No	No	No	No
MPC	No	No	No	No	No	Very little	No	No	No	Yes	No	No	No	No
MPC, EP	No	No	No	No	No	Very little	Somewhat	No	Yes	Yes	Yes	No	No	No
MPC, TEE, DP	No	No	No	No	No	No	Somewhat	No	Yes	Yes	Yes	No	No	No
MPC, DP, DP	No	No	No	No	No	Very little	Yes	No	Yes	Yes	Yes	No	No	No
MPC, TEE, DP, HE	Yes	Yes	No	No	No	Yes	Yes	No	No	No	No	No	No	No
MPC + 9 more	No	No	No	No	No	No	No	No	No	No	No	No	No	No
MPC, HE, DP, FL, SD	No	No	No	No	No	No	Yes	Somewhat	Somewhat	No	No	No	No	No
MPC, HE, DP, SD	No	No	No	No	No	No	No	No	No	No	No	No	No	No
MPC + 9 more	No	No	No	No	No	No	No	No	Yes	Somewhat	No	No	No	No
HE	No	No	No	No	No	No	No	No	No	No	No	No	No	No
General office	No	No	No	No	No	No	No	No	Yes	Somewhat	No	No	No	No
General office	No	No	No	No	No	No	No	No	No	No	No	No	No	No

Example: monitoring pre-school education



Read more at: <https://www.mpcalliance.org/blog/eus-vision-of-data-spaces-is-here>

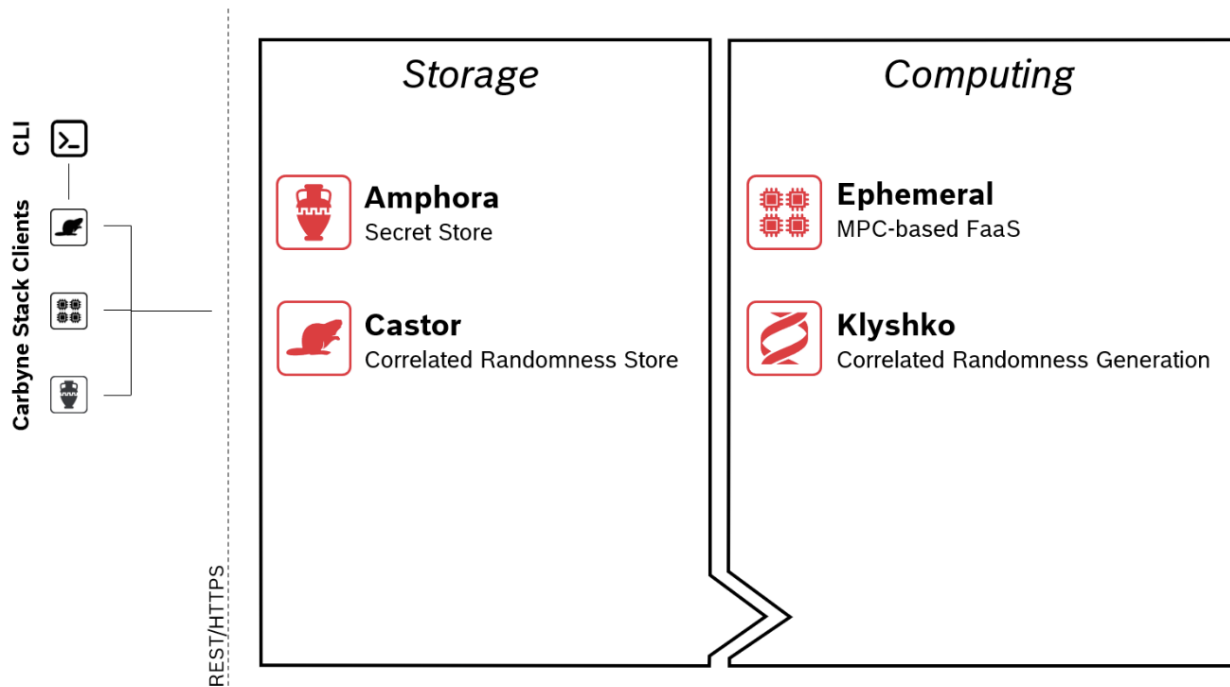
Example: WFA HALO Cross-Media Measurement



- MPC with differential privacy
- In innovative fashion, sought MPC node host providers publicly

Read more at: <https://wfanet.org/leadership/cross-media-measurement>

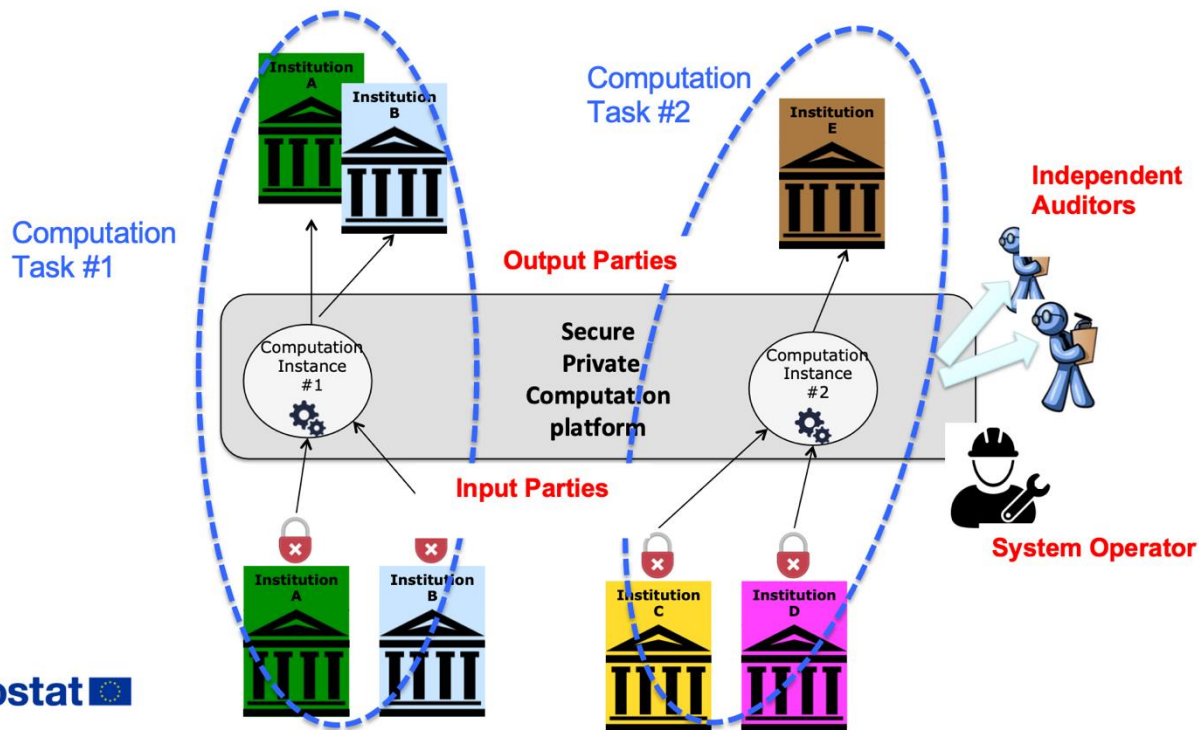
Carbyne Stack framework for cloud-native MPC



- Open source
- Seeks compatibility with multiple runtimes
- International community

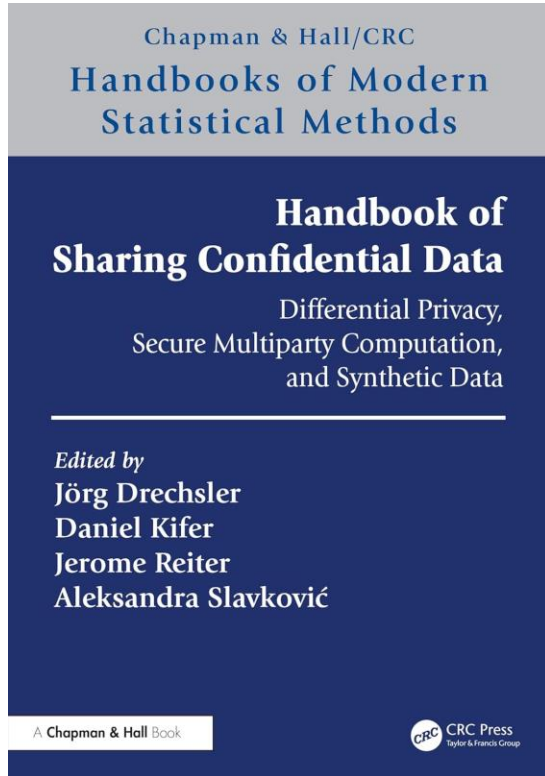
Learn more at: <https://carbynestack.io>

MPC for Trusted Statistics initiative from Eurostat



- Eurostat's PET work hub: <https://cros.ec.europa.eu/PET4OS>
- In 2023, Eurostat ran a [procurement](#) to prototype and test the Secure and Private Multi Party Compute as a Service platform with significant competition.
- This work is currently ongoing in the Joint On-demand COmputation with No Data Exchange (JOCONDE) project: <https://cros.ec.europa.eu/joconde>

New book on sharing confidential data (also with MPC)



Includes chapters on:

- Privacy-Preserving Distributed Computation
- Differential Privacy and Cryptography
- Overview of Secure Multi-Party Computation Applications in Health Research and Social Sciences

To be published in October 2024 and available at:

<https://doi.org/10.1201/9781003185284>



Thank You!

www.mpcalliance.org