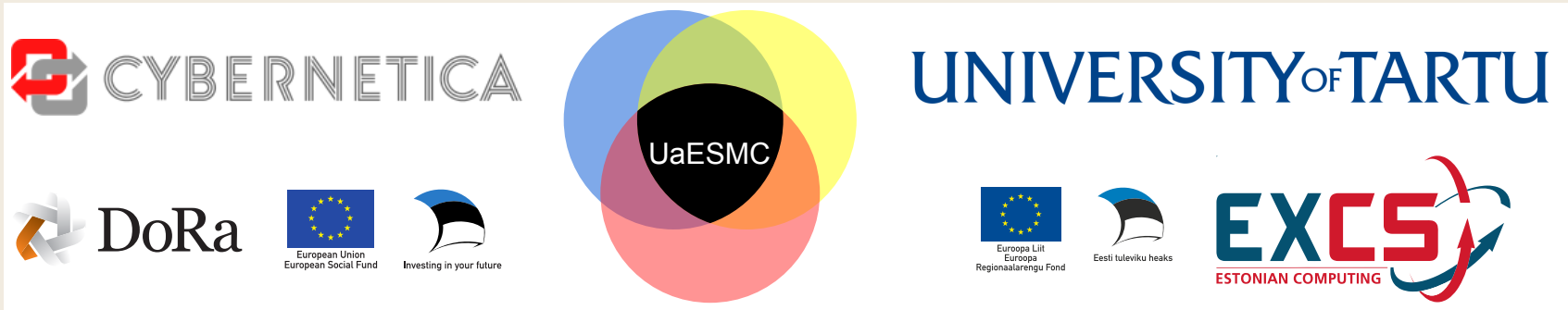
Privacy-Preserving Statistical Data Analysis on Federated Databases

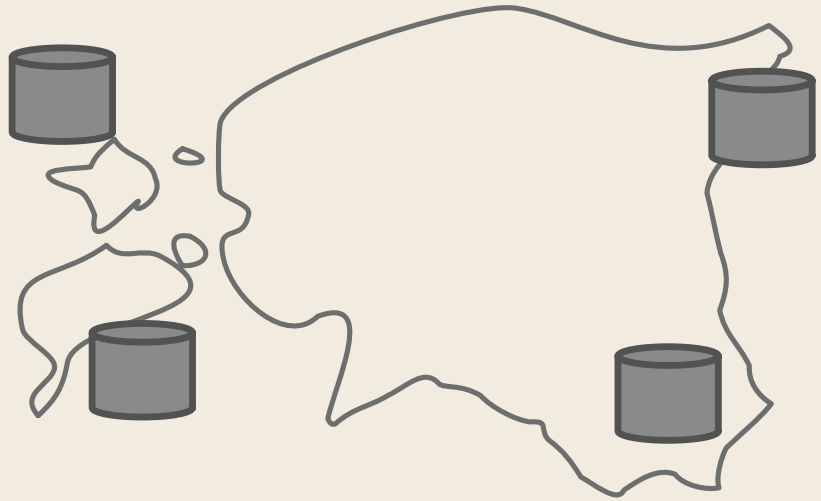
Dan Bogdanov Liina Kamm Sven Laur
Pille Pruulmann-Vengerfeldt Riivo Talviste Jan Willemson

Annual Privacy Forum
Athens, Greece
May 20, 2014



Problem Statement

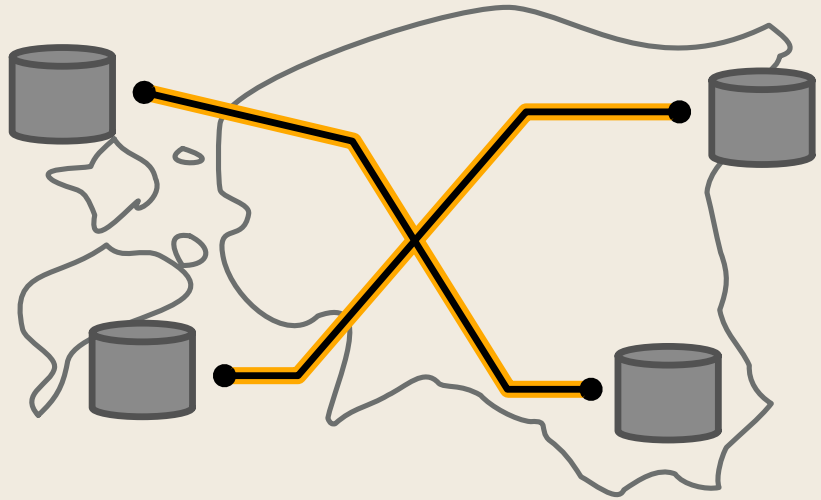
- State has many databases
- Many of these contain personally identifiable information (PII)



sharemind

X-Road Infrastructure

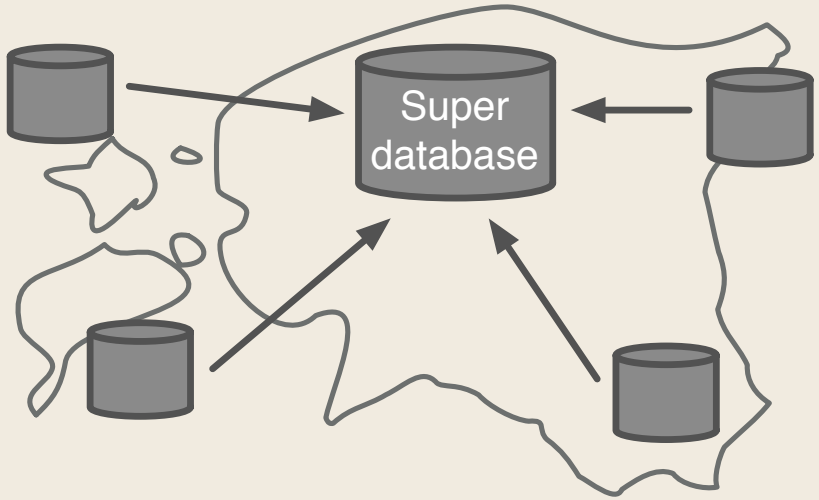
- Today, state databases are
  - interconnected by secure authenticated channels
  - interoperable using standardized protocols and data formats



sharemind

The Risks of Linking Databases

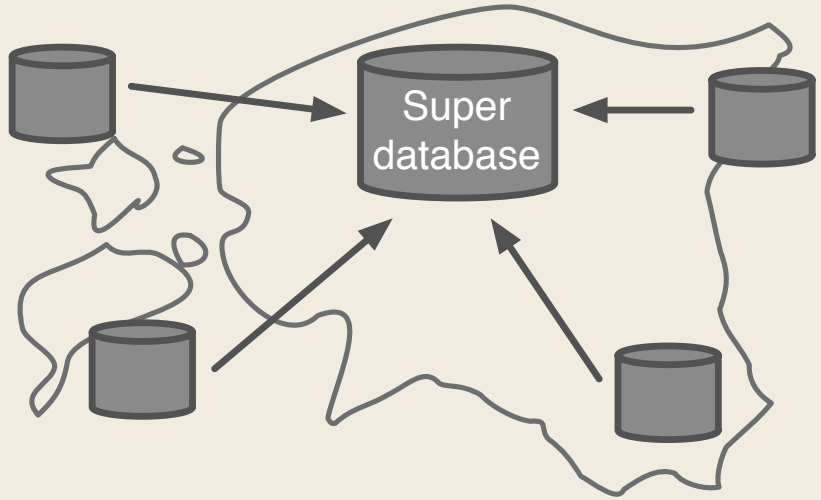
- Combining them would support state decisions



sharemind

The Risks of Linking Databases

- Combining them would support state decisions

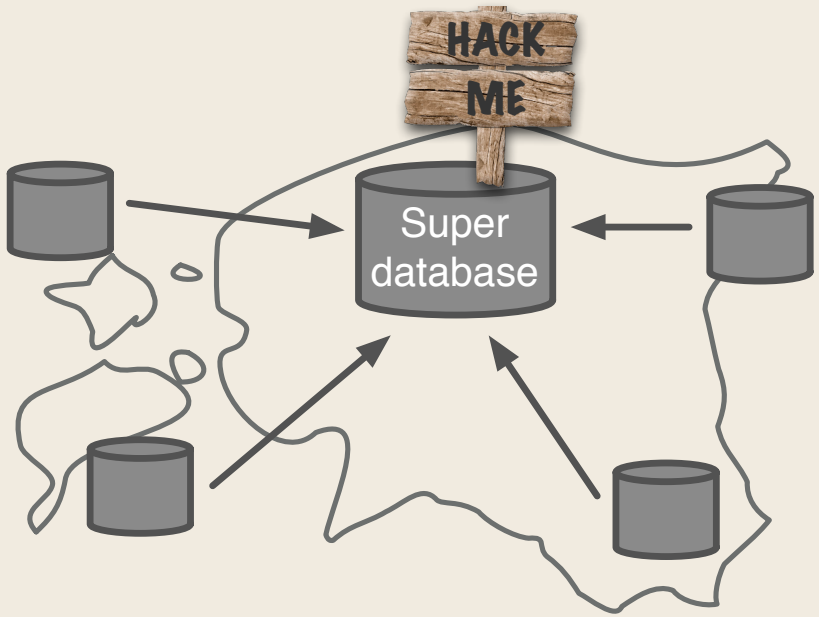


- Creating "super databases" is a privacy risk
  - Data is decrypted for analysis

sharemind

The Risks of Linking Databases

- Combining them would support state decisions

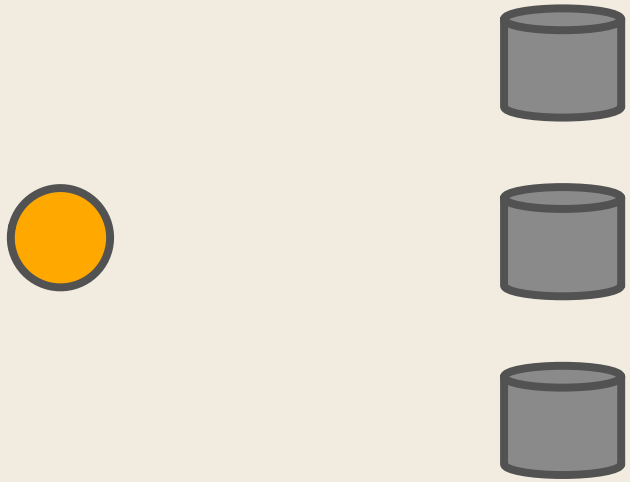


- Creating "super databases" is a privacy risk
  - Data is decrypted for analysis
  - Interesting target for attackers

sharemind

Secure Multi-party Computation

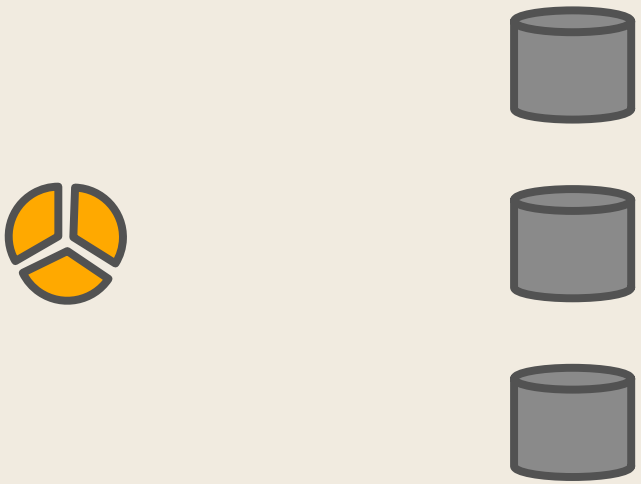
- Solution that does not require creating super database and preserves data utility
- Allows to compute on encrypted data
- All values are *secret shared*



sharemind

Secure Multi-party Computation

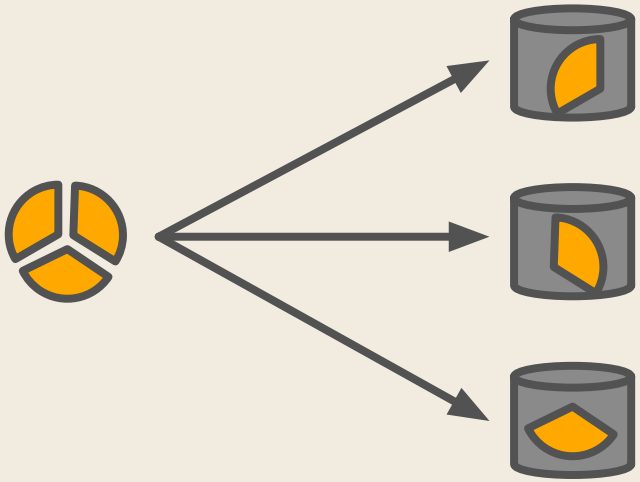
- Solution that does not require creating super database and preserves data utility
- Allows to compute on encrypted data
- All values are *secret shared*



sharemind

Secure Multi-party Computation

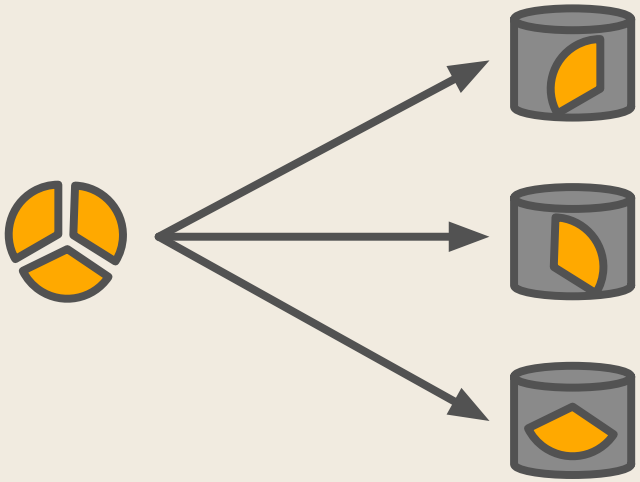
- Solution that does not require creating super database and preserves data utility
- Allows to compute on encrypted data
- All values are *secret shared*



sharemind

Secure Multi-party Computation

- Solution that does not require creating super database and preserves data utility
- Allows to compute on encrypted data
- All values are *secret shared*



- Distributed responsibility
  - No individual computation party has control over any inputs

sharemind

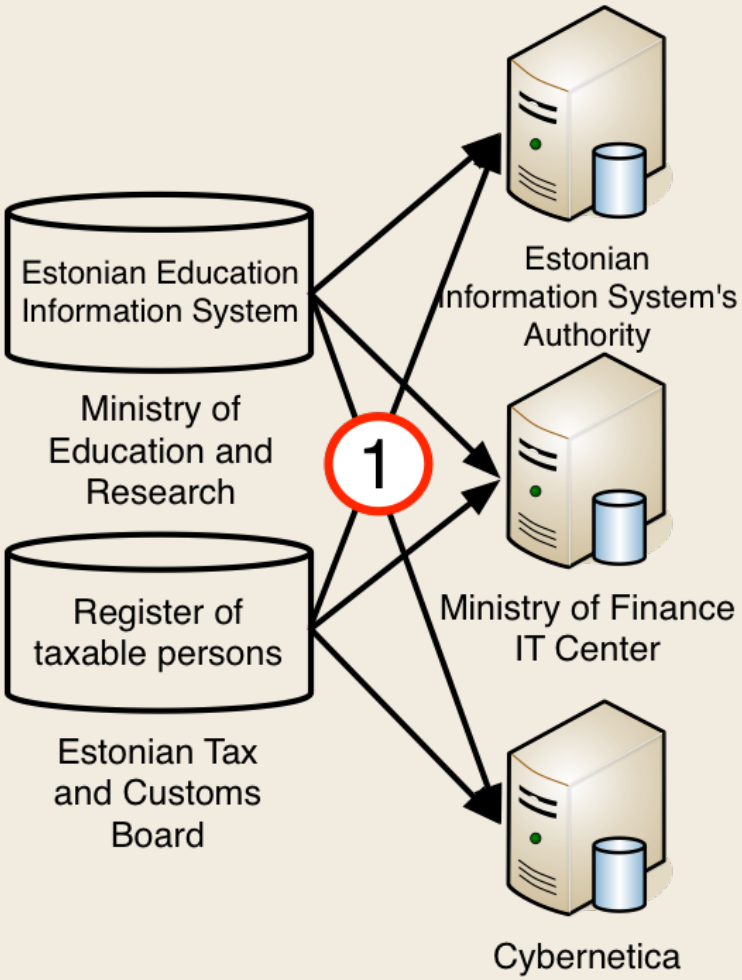
Our Practical Results

- We asked end-users whether they can see themselves using such a technology and the results were positive
- We used the Sharemind secure multi-party computation platform to implement a statistics suite
- Database linking is performed without declassifying the data
- We implemented a set of statistical functions and tests using Sharemind secure floating point operations

Privacy-Preserving Linking and Analysis

sharemind

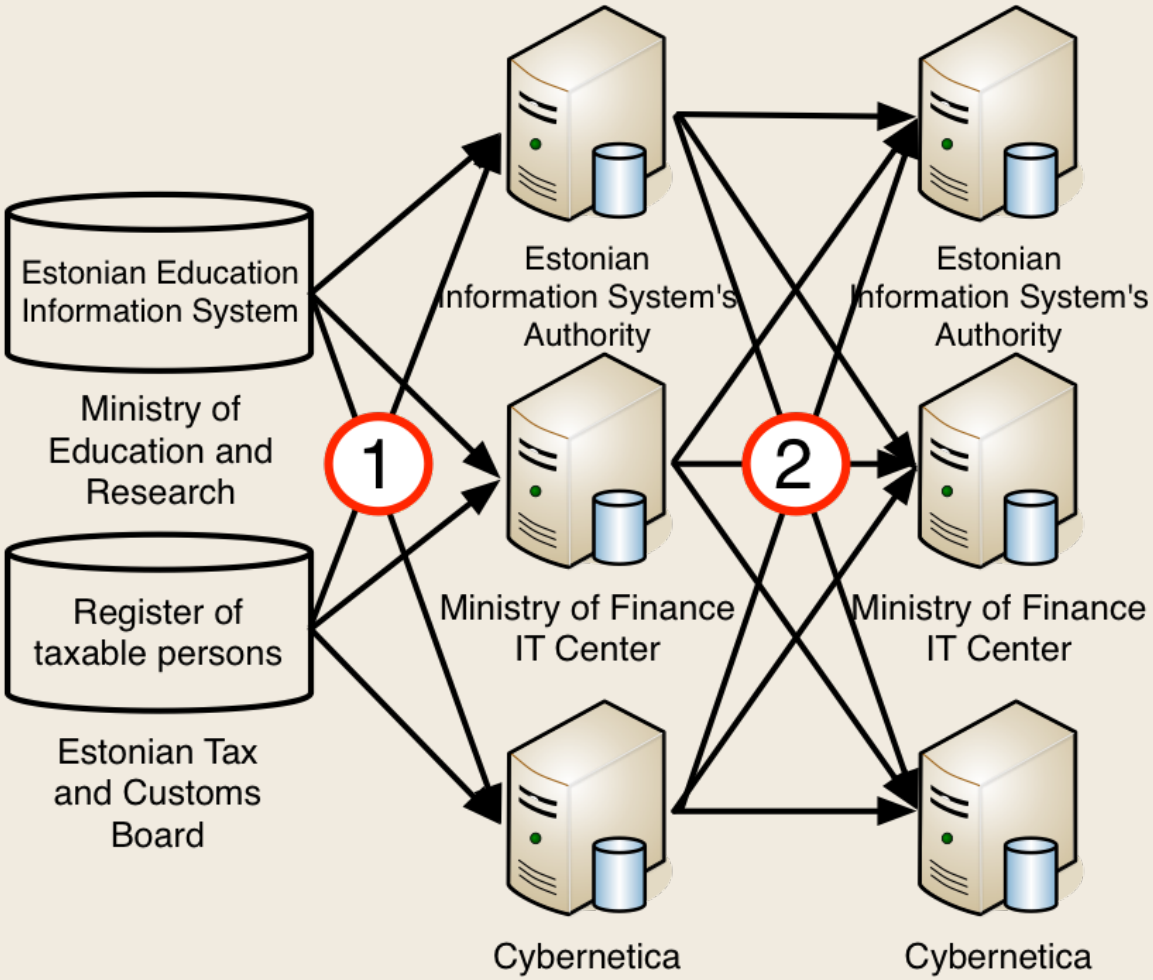
Privacy-Preserving Linking and Analysis



1 Encrypt and upload data

sharemind

Privacy-Preserving Linking and Analysis

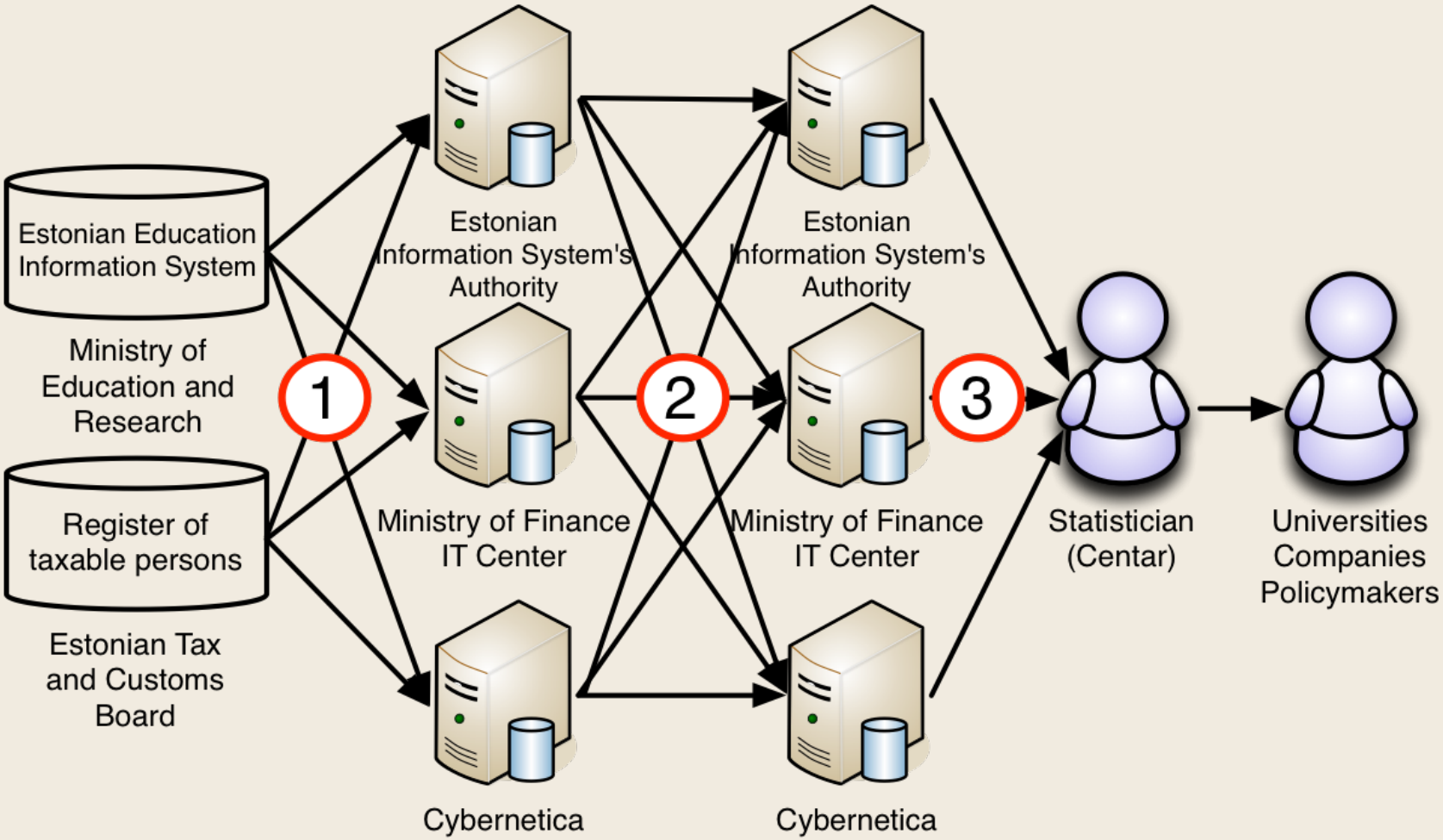


1 Encrypt and upload data

2 Analyse encrypted data

sharemind

Privacy-Preserving Linking and Analysis



1 Encrypt and upload data

2 Analyse encrypted data

3 Receive encrypted result and decrypt

sharemind

Future Work

The PRIST study will be carried out in the autumn of 2014.

Our goal is to help researchers, companies and governments understand the possibilities of secure multi-party computation technology.

We believe that secure computation can be used for sharing confidential data so that leaders in both private and public sectors can make better decisions without compromising privacy.

sharemind

Thank you!

https://sharemind.cyber.ee

The work of Riivo Talviste is supported by European Social Fund Doctoral Studies and Internationalisation Programme DoRa.

"Usable and Efficient Secure Multiparty Computation" (UaESMC) project is funded by the European Union Seventh Framework Programme for research, technological development and demonstration under grant agreement no FP7-284731. http://www.usable-security.eu/en

"Privacy-preserving statistical studies on linked databases" (PRIST) project is funded by the European Regional Development Fund through the Implementing Agency Archimedes Foundation.
http://cyber.ee/en/research/research-projects/prist/

The work of Jan Willemson is supported by Competence Centre in Electronics-, Info- and Communication Technologies (ELIKO). All research done by employees of Cybernetica AS is also supported by the European Regional Development Fund through Centre of Excellence in Computer Science (EXCS), and by the Estonian Research Council under Institutional Research Grant IUT27-1.

sharemind