

– Deploying privacy enhancing technologies in e-government

Liina Kamm

Cybernetica, Estonia



Established
in 1997



Roots in
academia
since 1960



200
employees
(11% PhD)



Architects
of the
e-Estonia
Ecosystem

Solutions

Digital identity



Inter-operability



Cyber security



Privacy enhancement



Naval awareness



Border surveillance



PET concept and roadmap for an e-government

In the beginning of 2023, Estonia conducted a research project on privacy enhancing technologies (PETs) to work out a concept and roadmap for deploying these technologies in e-government.

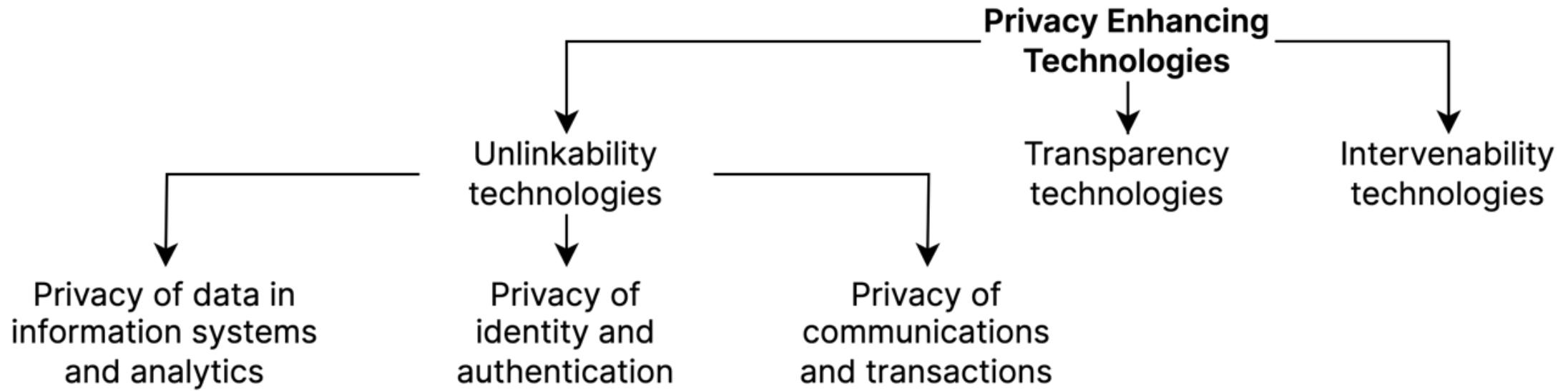
The PET concept for Estonia describes the technologies and provides a concept of generalised usage archetypes for the e-government.

The PET roadmap for Estonia describes the experiences of Estonian public sector organisations of using PETs in their work, their needs and requirements for data processing, and provides a roadmap for development and deployment of PETs in the public sector.

— Privacy enhancing technologies

What are privacy enhancing technologies?

Privacy enhancing technology is a privacy control, consisting of ICT measures, products, or services that protect privacy by eliminating or reducing PII or by preventing unnecessary and/or undesired processing of PII, all without losing the functionality of the ICT system. (ISO/IEC 29100:2011)



Data protection during analysis

- Pseudonymisation
- Anonymisation
- Restricted query interfaces
- Analyst sandboxes
- Differential privacy
- Federated learning
- Data synthesis
- Trusted execution environments
- Homomorphic cryptography
- Secure multi-party computation



Photo by Ryoji Iwata on Unsplash



Identity protection

- Blind signatures
- Group and ring signatures
- Attribute based cryptography
- Zero knowledge proofs

Anonymous communication

- Secure messaging
- Mixnets
- Onion routing

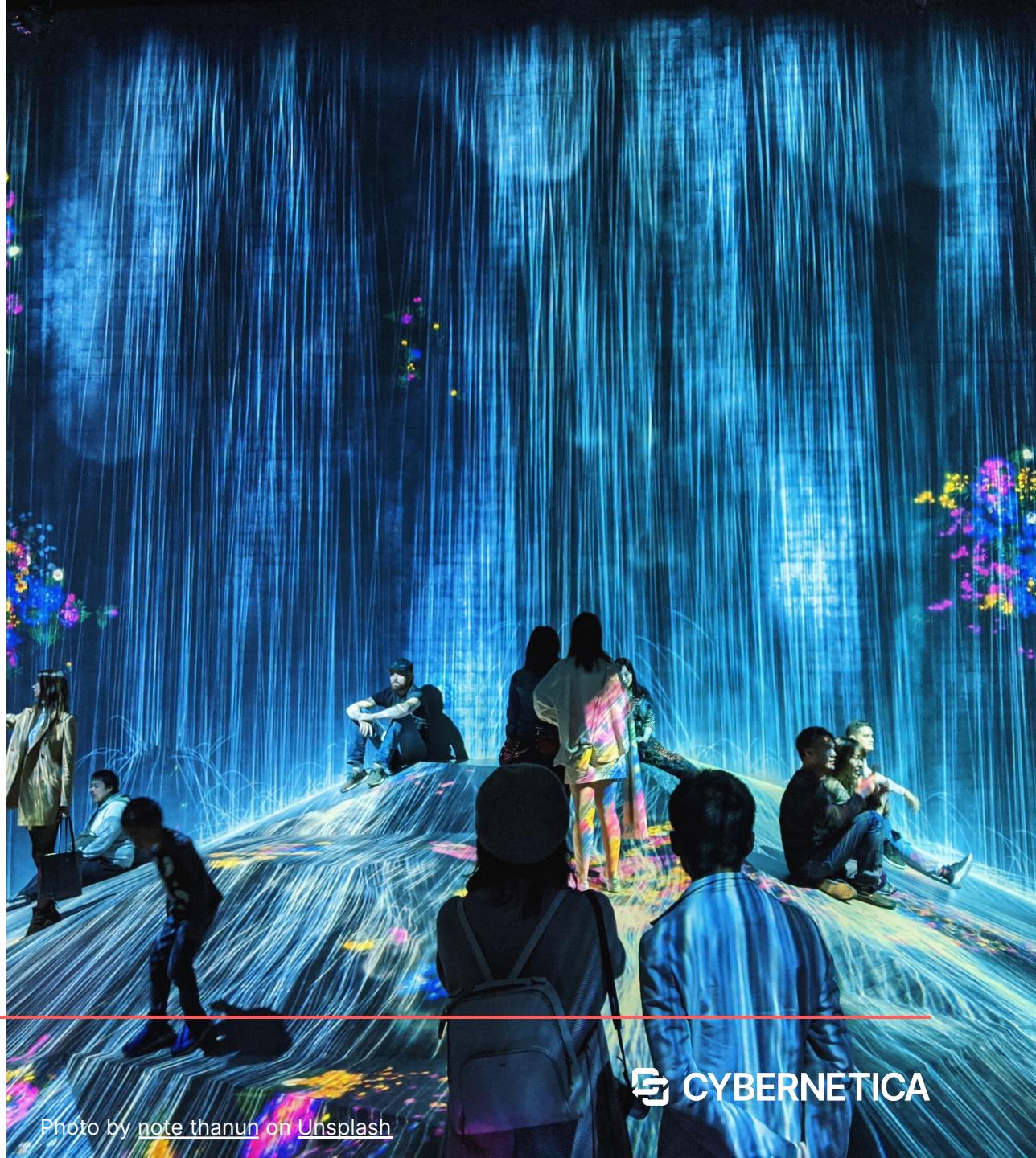
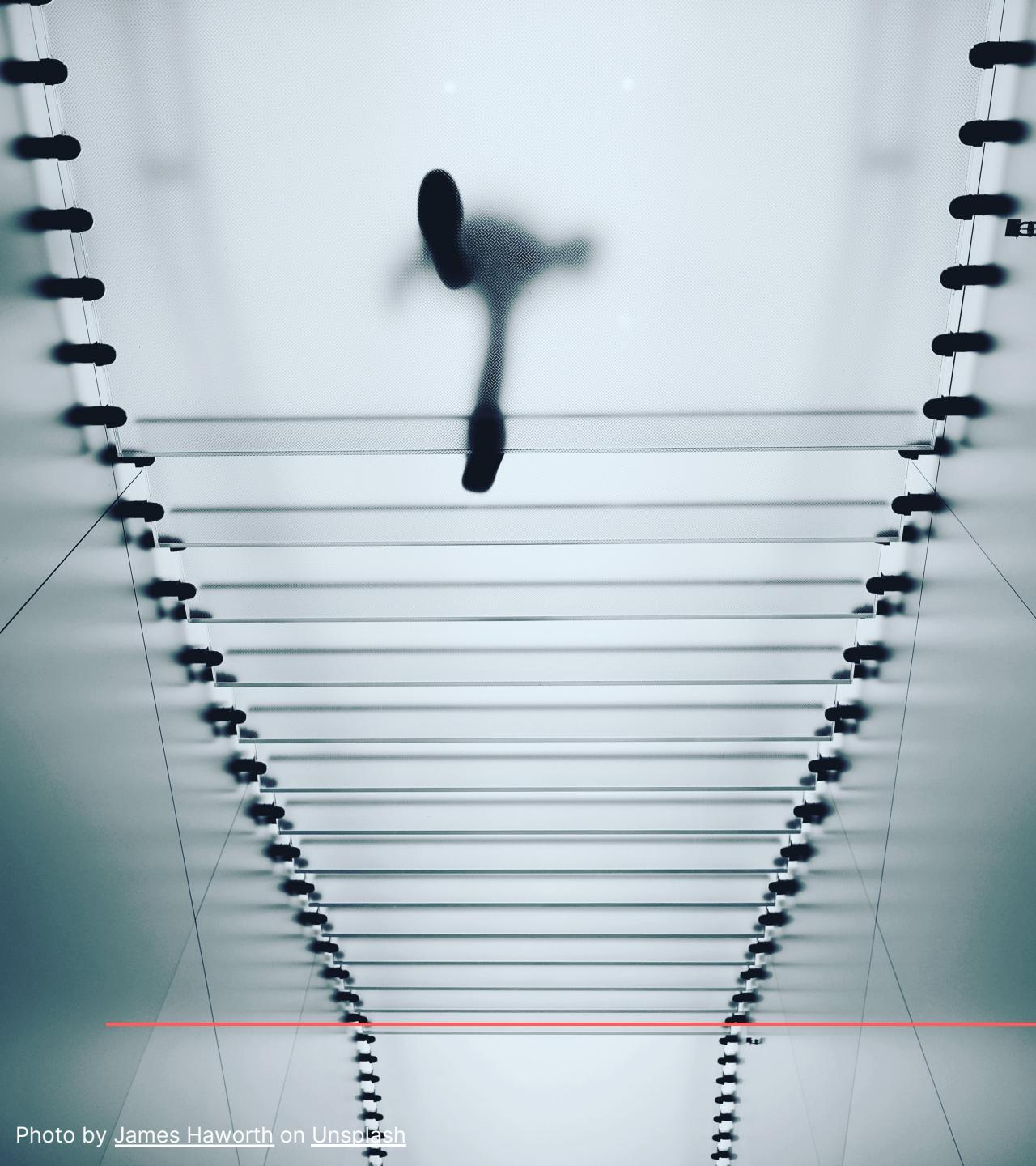


Photo by [note thanun](#) on [Unsplash](#)



Transparency and intervenability

Transparency

- Documentation
- Logging
- Notification of stakeholders
- Improving the understandability of terms and conditions

Intervenability

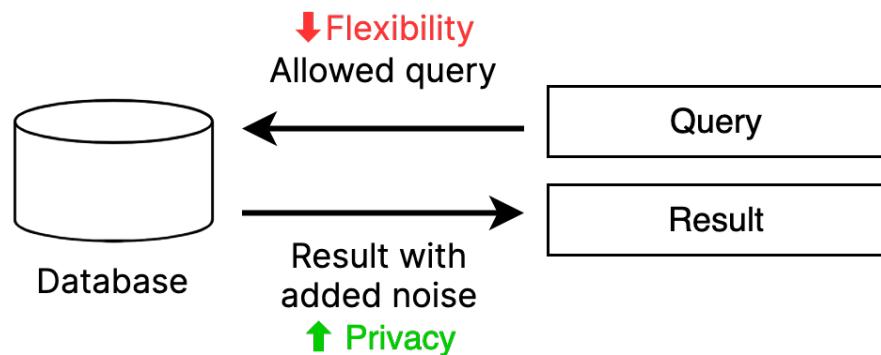
- Privacy and data processing panels and self service
- Dynamic consent management

Overview tables for each PET

Differential privacy

Short description: Differential privacy adds randomness to the query results so that the analyst cannot determine which individuals' data was included in the results.

Overview model:



Information

Complexity of development: high

Complexity of upkeep: low

Precision: not precise (depends on the noise)

Privacy guarantee: mathematically provable

Maturity: medium

Security assumptions and residual risk: ...

Legal considerations: ...

Possible use cases: ...

Known deployments: ...

Overview of deployments in the world

Examples and best practices from

1. The United States
2. The Netherlands
3. Japan
4. Canada
5. France
6. Singapore
7. The United Kingdom
8. Switzerland

Roadmap for the deployment of PETs

— Why should an e-government use PETs?

- PETs enable the creation of new services.
- PETs also protect corporate data.
- PETs support privacy-by-design.
- Estonian Digital Society Development Plan 2030:
Protection of fundamental rights, including privacy, is one of the principles of a digital society.
The evolution of a human-centred digital state is an opportunity for a digital developmental leap.

Interviews with 18 state agencies

1. Data Protection Inspectorate
2. Ministry of Justice
3. Ministry of Economic Affairs and Communications
4. Transport Administration
5. Estonian Tax and Customs Board,
6. The IT Centre of the Ministry of Finance
7. Ministry of Finance
8. Financial Supervision and Resolution Authority
9. Information System Authority
10. Ministry of the Interior
11. Police and Border Guard Board
12. Rescue Board
13. The IT of the Ministry of the Interior
14. Ministry of Social Affairs
15. Health and Welfare Information Systems Centre
16. Statistics Board
17. Estonian Genome Bank (Geenivaramu)
18. Healthcare Board (Tervisekassa)

Interview methodology

- How is privacy protection (or data protection) associated with your organization/sector's daily activities?
- What privacy protection solutions do you implement today, and why?
- Which challenges of your institution/sector (including cross-border cooperation) could be solved by using PETs and how would this (positively) impact Estonia and its people?

I'm so glad you asked!

“Our data analysts program in Python”

“Our data analysts work in Excel on data sets exported by our IT team”

“But we can already access all data!”

“But no external party has asked to analyse our data!”

“Are you going to make us use secure multi-party computation?”

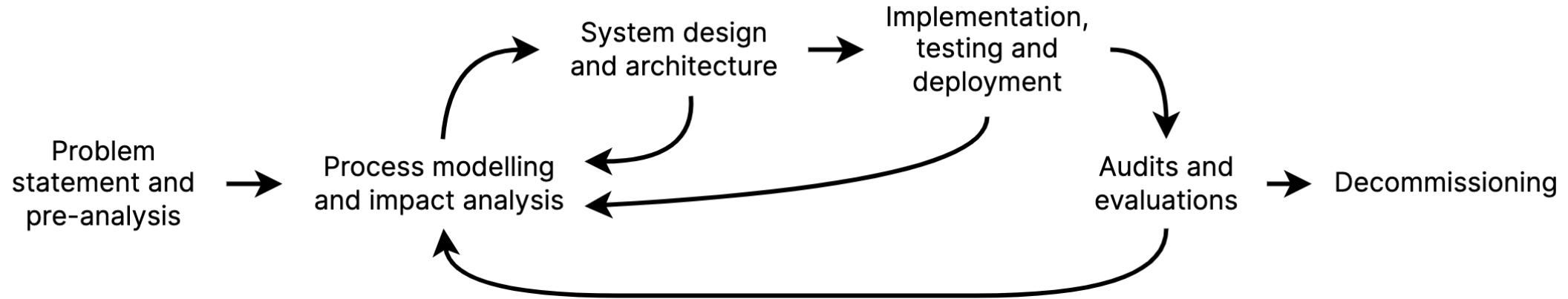
“This is too technical, why am I at this interview?”

“This is the exact level of abstraction that we need!”

“Here is a list of things that we want”

“How soon can you have this system ready?”

Privacy engineering in the system lifecycle



- In **new systems**, privacy engineering and PETs should already be incorporated at the **problem statement and requirements** stage.
- In **existing systems**, privacy engineering requirements should be added during **system redesigns**.

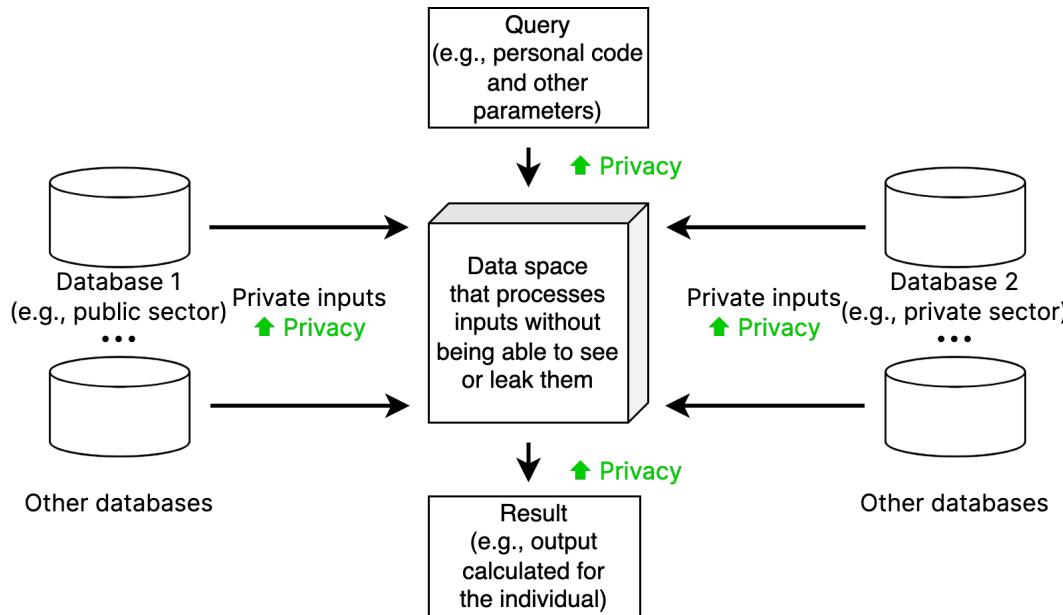
General use cases

- Secure data space for creating data driven services
- Privacy-preserving service for data linking and analysis
- Services based on open data
- Publishing a database as open data
- Synthetic digital twin of the state data and services
- Privacy-preserving logging and log analysis
- Proving attributes and/or properties

Secure data spaces

Secure data space for creating data driven services

Short description: Based on several (public or private sector) databases an individual is provided with an e-service.



Applicable privacy enhancing technologies:

1. Trusted execution environments
2. Secure multi-party computation
3. Homomorphic cryptography

Additional value created:...

Benefits of using privacy technologies: ...

Deployments:

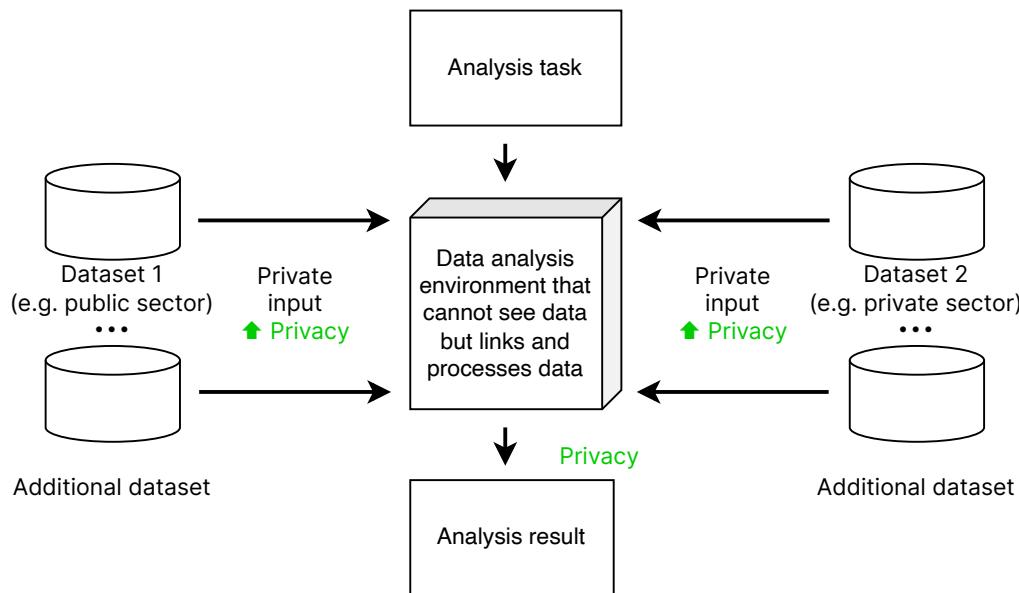
1. Proactive subsidies
2. Inclusion of health data from private sector health providers into government services
3. Positive credit registry
4. Digital accommodation forms

Example applications: ...

Data linking and analysis

Privacy-preserving service for data linking and analysis

Short description: Data from multiple sources is collected, linked and analysed using PETs to create new models and insights.



Applicable privacy enhancing technologies:

1. Secure multi-party computation
2. Trusted execution environments
3. Federated learning (no linking)
4. Homomorphic cryptography
5. Additional output privacy measures as needed

Additional value created:...

Benefits of using privacy technologies: ...

Deployments:

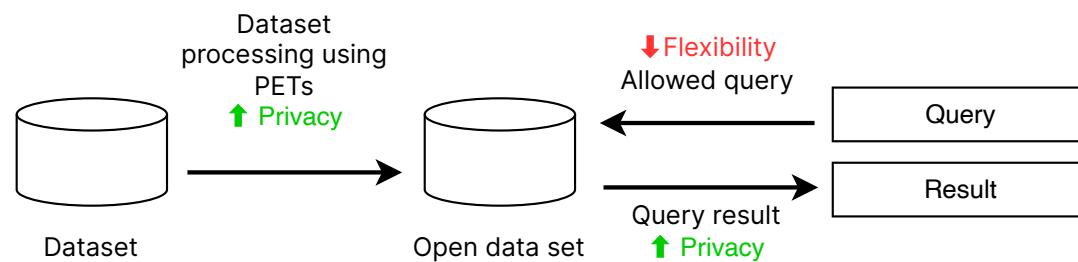
1. Investigating financial fraud
2. Positive credit registry
3. Analysis of digital accommodation cards
4. Mobility data analysis

Example applications: ...

Services based on open data

Services based on open data

Short description: A state database is queried in a limited fashion as a data source for the construction of services.



Applicable privacy enhancing technologies:

1. Restricted query interfaces
2. Differential privacy
3. Data synthesis
4. Anonymisation
5. Additional output privacy measures as needed

Additional value created:...

Benefits of using privacy technologies: ...

Deployments:

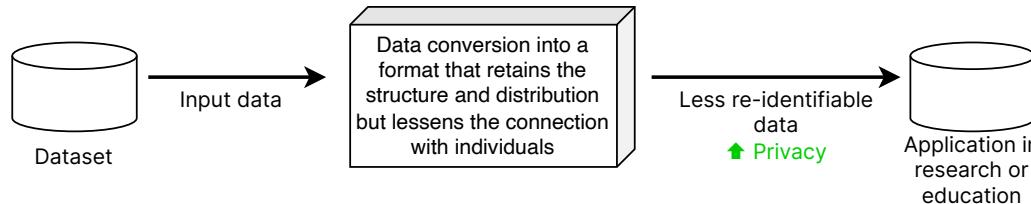
1. Open data services in education, healthcare, finance, transport, energy

Example applications: ...

Publishing a database as open data

Publishing a database as open data

Short description: A state dataset is processed using PETs and provided to the user in for use in teaching, research or testing. The database may be made completely public or given to a limited number of users.



Applicable privacy enhancing technologies:

1. Data synthesis
2. Differential privacy
3. Anonymisation
4. Analyst sandboxes (only for research and teaching)
5. Additional output privacy measures as needed

Additional value created:...

Benefits of using privacy technologies: ...

Deployments:

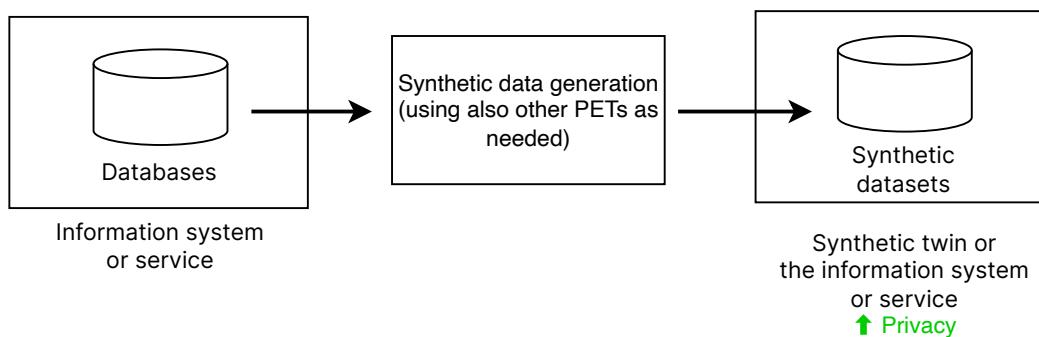
1. Publishing aggregated data (statistics)
2. Publishing health, finance, energy data for research

Example applications: ...

Synthetic digital twin

Synthetic digital twin of the state data and services

Short description: Copies of state services and the related datasets are created using PETs



Applicable privacy enhancing technologies:

1. Data synthesis
2. Secure computing technologies for data linking before synthesis

Additional value created:...

Benefits of using privacy technologies: ...

Deployments:

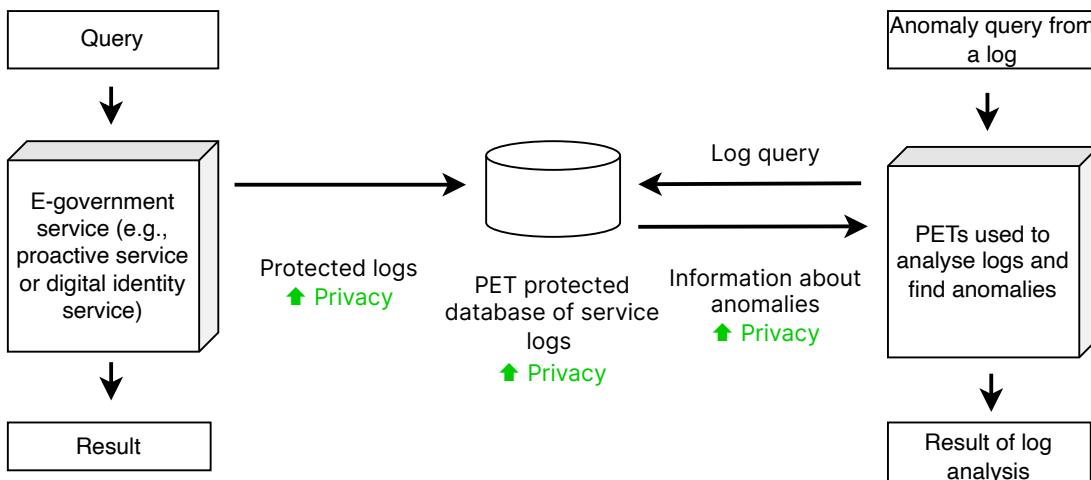
1. Synthetic digital twins for healthcare, finance, or other domains

Example applications: ...

Logging and log analysis

Privacy-preserving logging and log analysis

Short description: To avoid excessive profiling of users, PETs are used for logging, analysing logs and searching for anomalies or fraud.



Applicable privacy enhancing technologies:

1. Trusted execution environments
2. Secure multi-party computation
3. Homomorphic cryptography

Additional value created:...

Benefits of using privacy technologies: ...

Deployments:

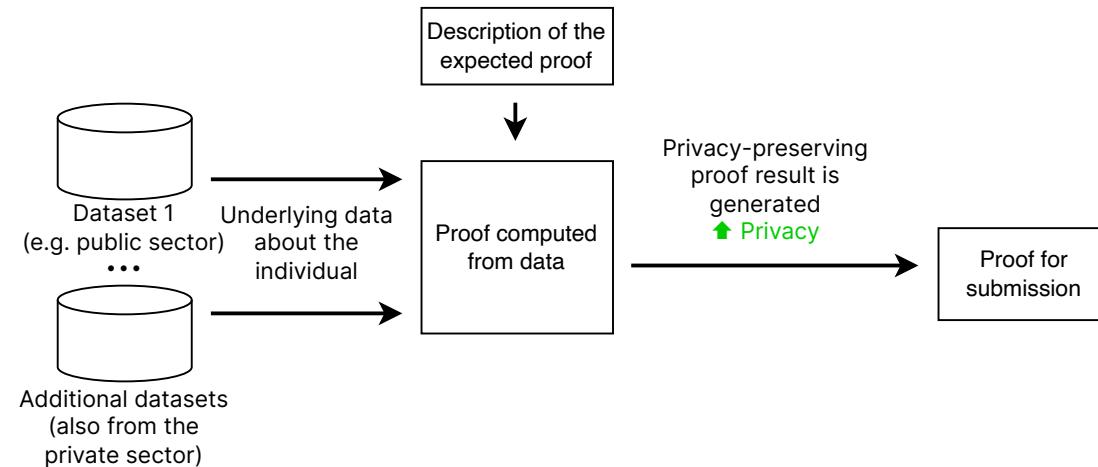
1. Protection of digital identity authentication logs and identification of anomalies
2. Proactive service log protection and identification of anomalies

Example applications: ...

Proving attributes and/or properties

Proving attributes and/or properties

Short description: Digital wallets and identities may allow people to prove that they are older than a certain age that they belong to a group, or they have a certain data element in the wallet.



Applicable privacy enhancing technologies:

1. Zero-knowledge proofs
2. Blind signatures
3. Group signatures

Additional value created:...

Benefits of using privacy technologies: ...

Deployments:

1. Proving one's age
2. Proving the mileage and location of electric vehicles
3. Proving compliance to health standards
4. Proving income or income source attributes

Example applications: ...

Policy recommendations regarding data

- Synthetic data and digital twins for software development
- Avoiding unnecessary double data requests
- Increasing data quality
- Data cleaning
- How to create open data
- Legal considerations and processes of big data
- Data management and handling during a crisis or war

Other policy recommendations

- Raising awareness about privacy and PETs in the general population and in the public sector
- How to choose the right PET and how to assess its appropriateness for the application (comparison and risk assessment)
- Resources needed for the uptake and deployment of PETs (finances and people; automating processes)
- Changing public sector process flows; more active networking and dissemination in Europe

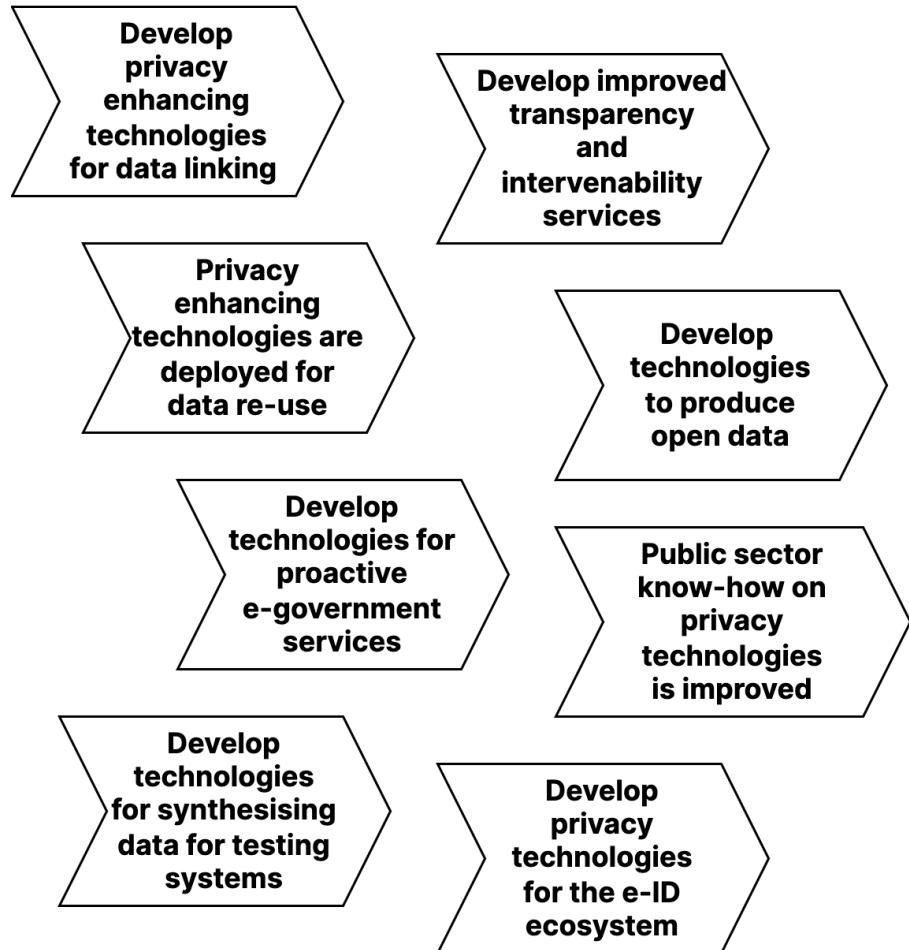
Main systems on the roadmap

Concept	Applications	Added value
Platform for personalised proactive services	<ol style="list-style-type: none">Personalised subsidiesProactive services on special category data	<ol style="list-style-type: none">Including data from the private sectorSaving by using more detailed dataEasier implementation of similar services
Platform for cross-database analytics	<ol style="list-style-type: none">Event preventionDevelopment of new servicesPolicy analysis	<ol style="list-style-type: none">Mitigating risks when population based datasets need to be linkedInvolving data from the private sector and analysts from the private sector and abroad
Reducing the risk of re-identification of open data	<ol style="list-style-type: none">Development of new servicesResearch and learning	<ol style="list-style-type: none">Measuring and comparing the probability of re-identificationProtecting against long term and linking attacks
Digital identity (eID) logs and analytics	<ol style="list-style-type: none">Logging and analytics of confirmation of authentication and validity	<ol style="list-style-type: none">Achieving eIDAS 2.0 data protection requirementsPreventing profiling
Synthetic digital twin of the e-government	<ol style="list-style-type: none">Developing and testing services	<ol style="list-style-type: none">Faster development and testing of new systemsPreventing the use of personal data in development and testing

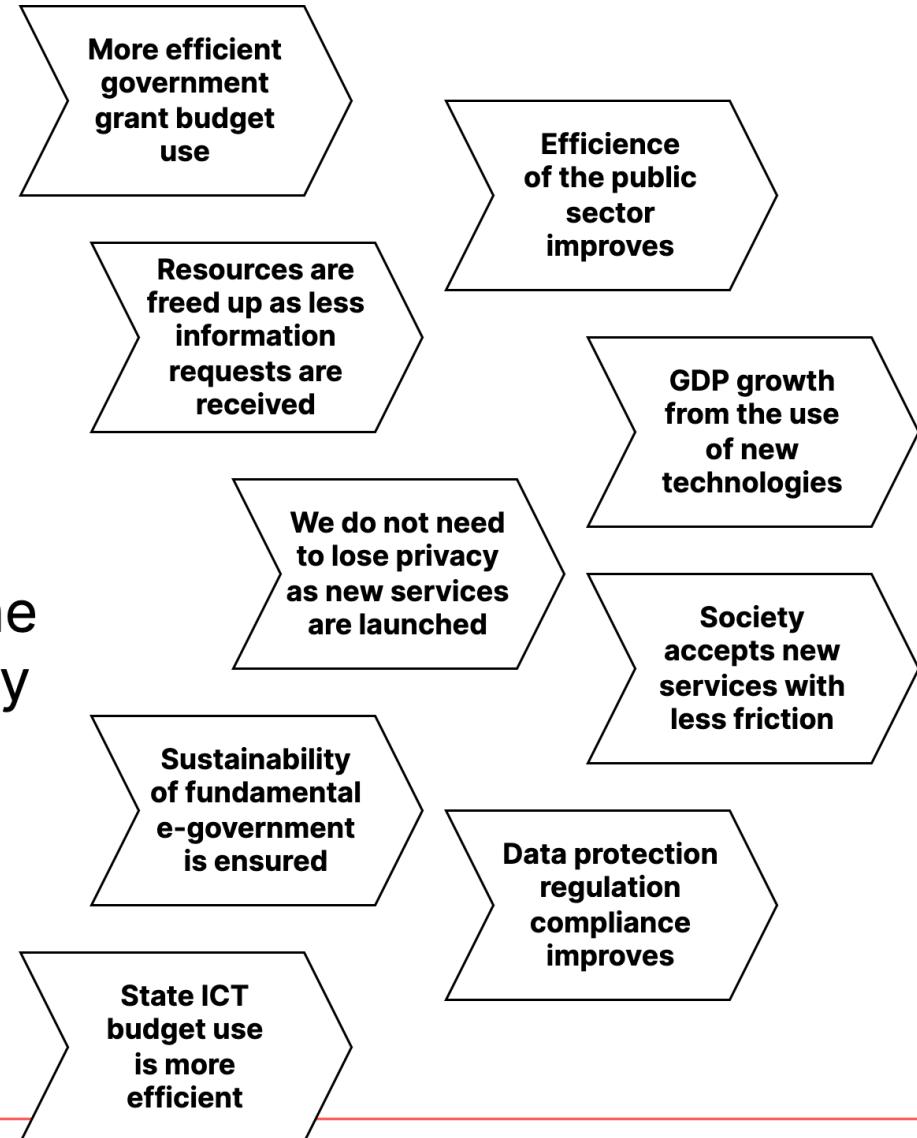
Roadmap

Action	Stage	Result	Performance indicators	Start	Possible implementer
Platform for personalised proactive services	Innovation	Architecture and prototype	5 services included	2023	Government office, Information Systems Authority
Platform for personalised proactive services	Pilot project	Deployed pilot service	1 service implemented using a PET	2024	Information Systems Authority
Platform for personalised proactive services	Creation and reuse of a platform	A platform for creating secure business applications; integration with X-Road and eID	1 platform for implementing services using PETs; 5 services implemented using PETs	2025+	Information Systems Authority
...

Value chains



Privacy
Enhancing
Technology
program in the
Digital Society
roadmap



Learn Estonian today!

- PET overview: <https://mkm.ee/sites/default/files/documents/2023-04/Privaatsuskaitse%20tehnoloogiate%20kontseptsioon.pdf>
- PET roadmap: <https://mkm.ee/sites/default/files/documents/2023-04/Privaatsuskaitse%20tehnoloogiate%20Eestis%20rakendamise%20teekaat.pdf>
- Page with all results: <https://www.kratid.ee/analuusid-ja-uuringud#pet>

— Thank you!

Liina Kamm

liina.kamm@cyber.ee

 <https://cyber.ee/>

 info@cyber.ee

 [cybernetica](https://twitter.com/cybernetica)

 [CyberneticaAS](https://facebook.com/CyberneticaAS)

 [cybernetica_ee](https://instagram.com/cybernetica_ee)

 [Cybernetica](https://linkedin.com/company/cybernetica)