# Privacy-Enhancing Cryptology in the Swedish Public Administration

Alexander Engström,
The National Defence Radio Establishment / Försvarets Radioanstalt, Sweden
alexander.engstrom@fra.se

Erik Janzon,
The Swedish Social Insurance Inspectorate / Inspektionen för socialförsäkringen

Integritetsfrämjande teknik i offentlig förvaltning, SOU 2026:44

Talk at NIST WPEC 2026 on October 26, 2026.

# Introduction

- Public administrations face a fundamental tension: the urgent need for data-driven decision-making and AI training versus the strict constraints of data protection laws (such as GDPR in the EU) and national security acts.
- Traditional methods of anonymization often fail to balance data utility with privacy, creating “data silos” that hinder socio-economic growth.
- This presentation explores the implementation of a national infrastructure in Sweden designed to bridge this gap through the deployment of advanced cryptographic PETs.



# The Inquiry

- This type of inquiry committee appointed by the Swedish government is required before new laws are proposed. The essential question: Should any laws be changed to increase the adaptation of PETs in the Swedish public administration.
- A one year long inquiry chaired by Erik Janzon, the Director General of the Swedish Social Insurance Inspectorate.
- Four legal scholars and one cryptologist on the committee. Several consultants and expert groups representing agencies, companies and public interest groups involved.
- The final report is at: https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2026/06/sou-202644/
- It's 400 pages in Swedish, with an English summary on pp 23-30.
- Specific techniques: pp. 61-84; Standards: pp. 119-130.



# Standardization implications for our use cases

- Secure Multi-Part Computation, Private Set Intersection, and similar: Standardize modular components that allow for small decision trees with input from several parties.

- Zero-Knowledge Proofs: Standardization (for EU projects) is urgently needed. Everything do not need to be quantum-safe now. But document it extraordinary well.

- Homomorphic encryption: Very long-term, it is easier (in Sweden) to legally analyze and approve complex information systems if data is always encrypted rather than protected by TEEs or similar. Make it abundantly clear for lawyers when everything is encrypted.

- Security levels: In the governmental setting some security is provided by other means than the PEC, compared to on the Internet. Standardized ”low” PEC security levels may increase governmental adaptation thanks to more reasonable costs.

# Secure Multi-Part Computation, Private Set Intersection, and similar…

# Use case: Secure Multi-Part Computation, PSI,…

- Agency A has the monthly income data per person
- Agency B has the housing benefits data per person
- The agencies are not allowed to transfer that data between each other due to privacy concerns.

- Welfare state use case: Some of the most vulnerable citizens do not apply for benefits, although they meet the requirements and it is known from other inquiries that the effect is really good in that group.
- Solution: Calculate the intersection of {Persons with low income} and {Persons with no housing benefits} using PSI and pre-approve them.

- Law enforcement: Some persons lie about their income.
- Solution: Calculate the intersection of {Persons with high income} and {Persons with housing benefits} using PSI and forward that list to law enforcement.

# Use case: Secure Multi-Part Computation, PSI,…

- The inquiry proposes that a governmental agency will create and run the infrastructure for other agencies to perform PSI-calculations and similar.
- We want those calculations to build on PEC-standards. In particular, that will allow for procurement on an international market rather than in-house development. Good for implementation security and costs.

- We need standards that are slightly more involved than PSI!
- Think of data from 4-5 agencies, perhaps 2-3 numbers and 2-3 boolean variables. That data is processed in a small decision tree, and we save the name of everyone that the decision tree singles out.
- The decision trees change very seldom, perhaps on a yearly basis. (They are based on legal rules and thresholds decided on paper by agencies; not AI-produced)

- At the moment, we don’t believe that a standard for homomorphic encryption will solve this. In theory it does, but it’s too slow and the procurement of a generic solution is too far off from the use cases and requires too much in-house expertise. Optimally, an expert on the decision tree rules should be able to piece everything together without any IT expertise.

- The inquiry proposed that the Swedish Tax Authority should host this SMPC service.

# Zero-Knowledge Proofs

# Zero-Knowledge Proofs

- Lots of activity within the EU framework: Wallets and data spaces. The inquiry highlighted solutions for health data.

- Everything do not need to be quantum-safe right now!
- For several use cases it's better right now to have a standardized non-quantum-safe solution rather than a non-standardized quantum-safe solution
- Work with different time-lines for ZKP-standardization, and how to incorporate that in crypto-agility for PECs.
- The alignment between PQC transition roadmaps and PEC standardization could in general be better, as discussed at IETF.

# Homomorphic encryption

# Homomorphic encryption

- In the inquiry chapter on the future of PETs, there is a section on *Encryption as a rule*.
- From a legal standpoint, in Sweden, it's easier to analyze an information system where everything is encrypted all of the time.
- A computation involving sensitive personal data done in cleartext protected by a TEE compared to under encryption by homomorphic encryption, are very different legally.
- The inquiry speculate in a future, several decades a head, where encryption as a rule is mandatory for certain areas.
- Standards should make it very clear when everything is encrypted, even to a lawyer reading the introduction of a standard during a procurement process. Challenge: Explain transciphering to a legal scholar, or just bootstrapping — why is the encryption not lost?

# Security levels

# Security levels

- Our inquiry was mainly on the use of PETs between governmental agencies
- They already have lots of security based on ordinary cryptology, and rules and regulations regarding that
- Several PECs are expensive in computer time. Standards for them should allow for that certain security measures are solved by other means, for example ordinary cryptology
- That is, if certain privacy or security aspects of a PEC technology may be solved by another technical tool, it may be advantageous to leave that out of the spec as a requirement. Or allow for a ”low” PEC security that in practice requires a complementary, but less expensive, other risk management action.

# Thank you!

alexander.engstrom@fra.se