Advanced cryptography for privacy protection

Cases from the government field

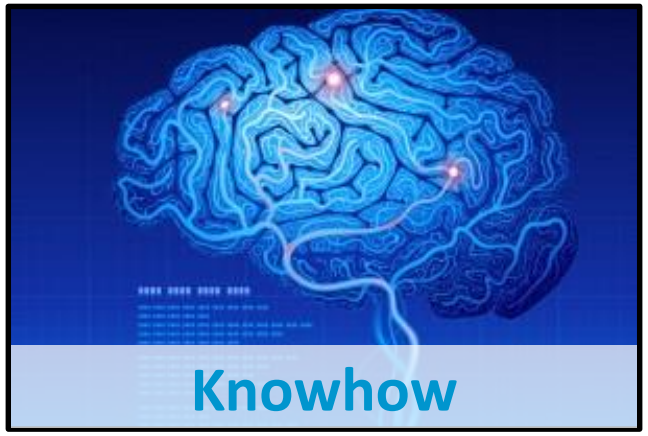
Kristof Verslype
PhD, Smals Research

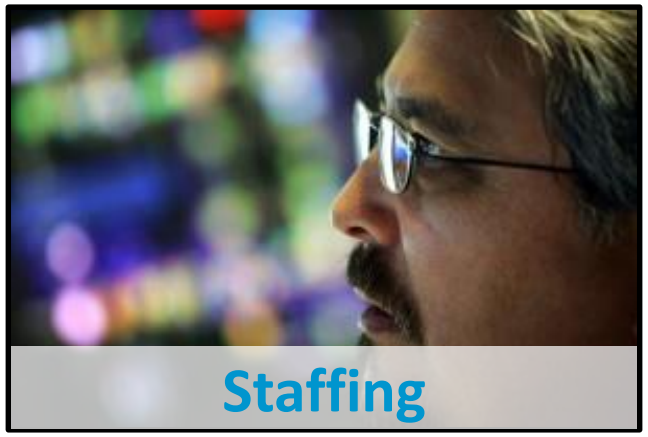
20 dec. 2019

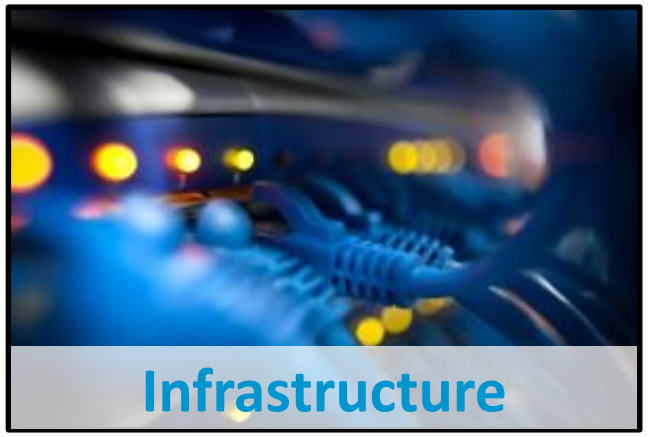
Smals
ICT for society

Smals
ICT for society

SUPPORT FOR E-GOVERNMENT







g-cloud

top EMPLOYER BELGIË BELGIQUE
CERTIFIED EXCELLENCE IN EMPLOYEE CONDITIONS

WWW.SMALS.BE

Smals
ICT for society

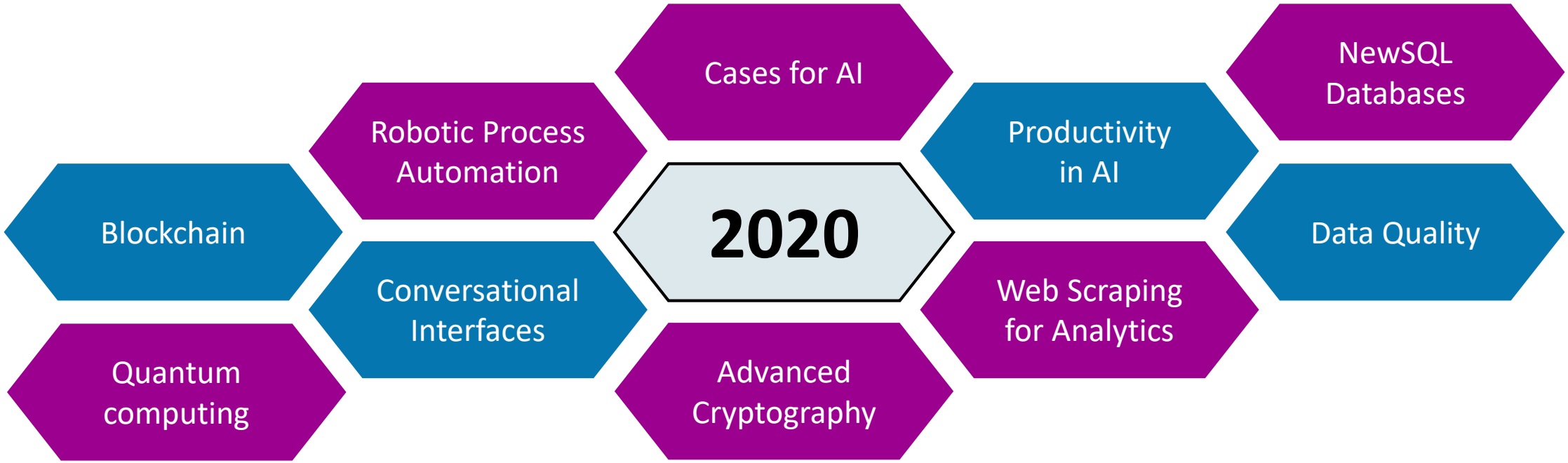
Smals Research

Innovation with new technologies

Consultancy & expertise

Internal & external knowledge transfer

Support for going live



www.smalsresearch.be

Smals ICT for society

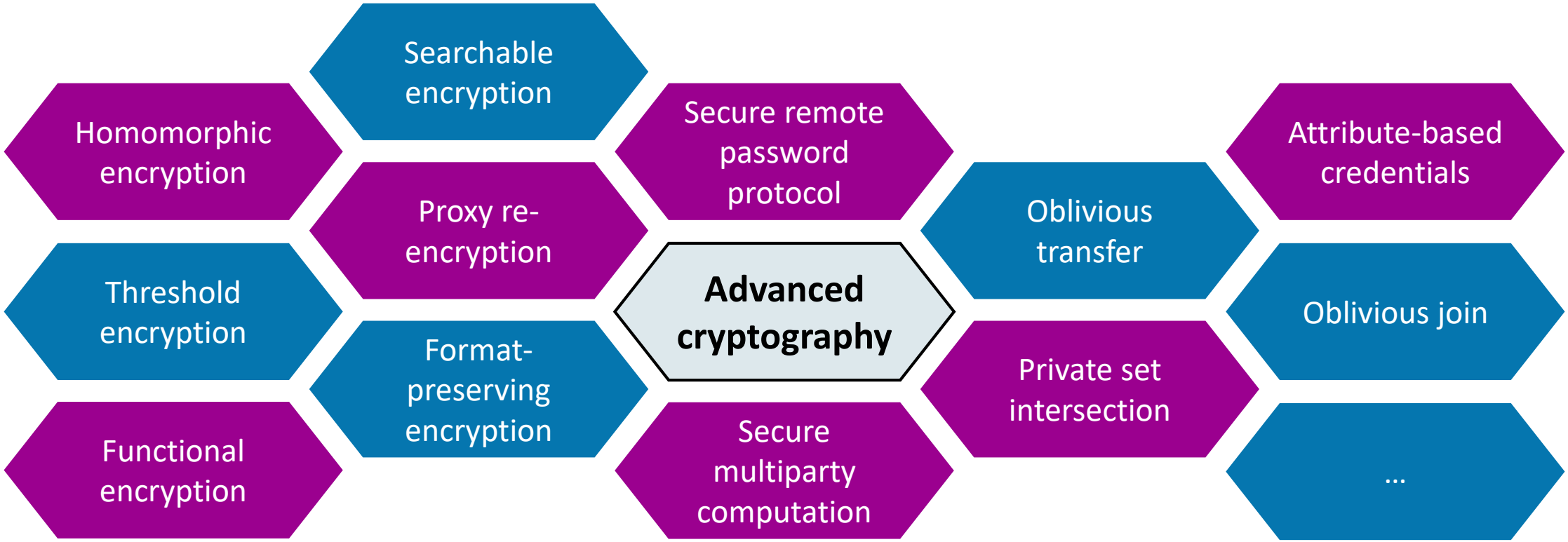
Much more is possible with cryptography

CRYPTO WORK HORSES

- Symmetric encryption
- Digital signatures
- Public key cryptography
- Hashing
- Authentication
- …

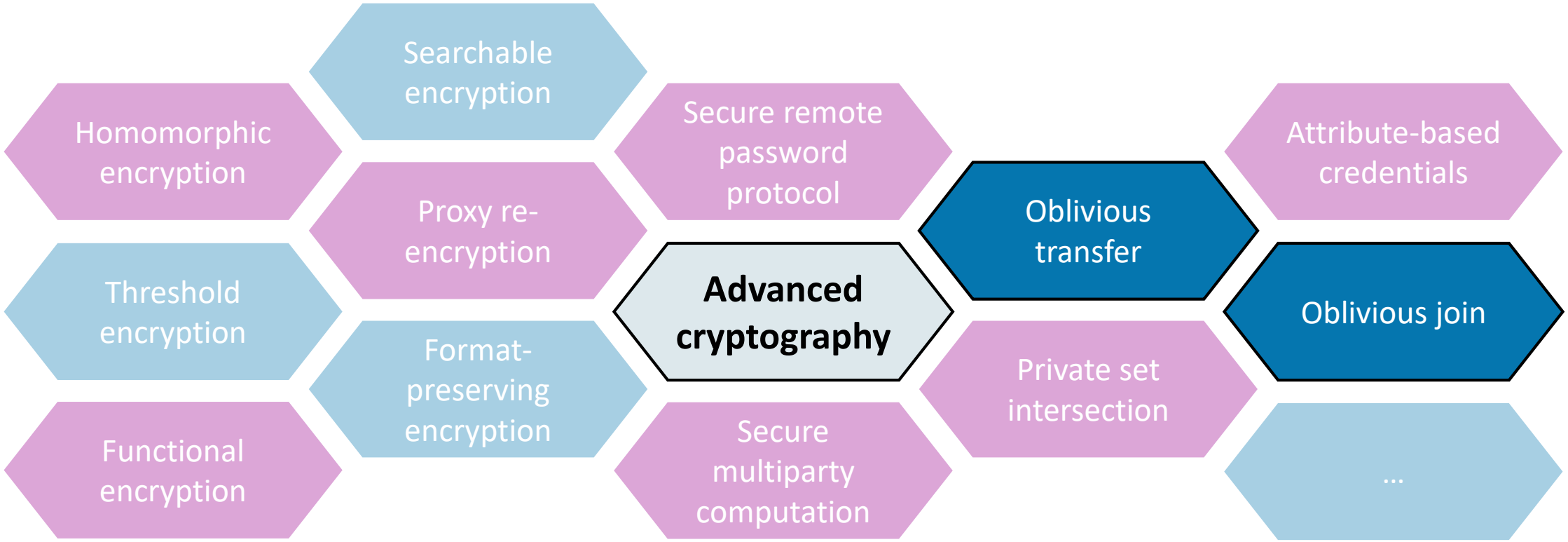
Known & widely applied in government context

Advanced cryptography



Potential within government context

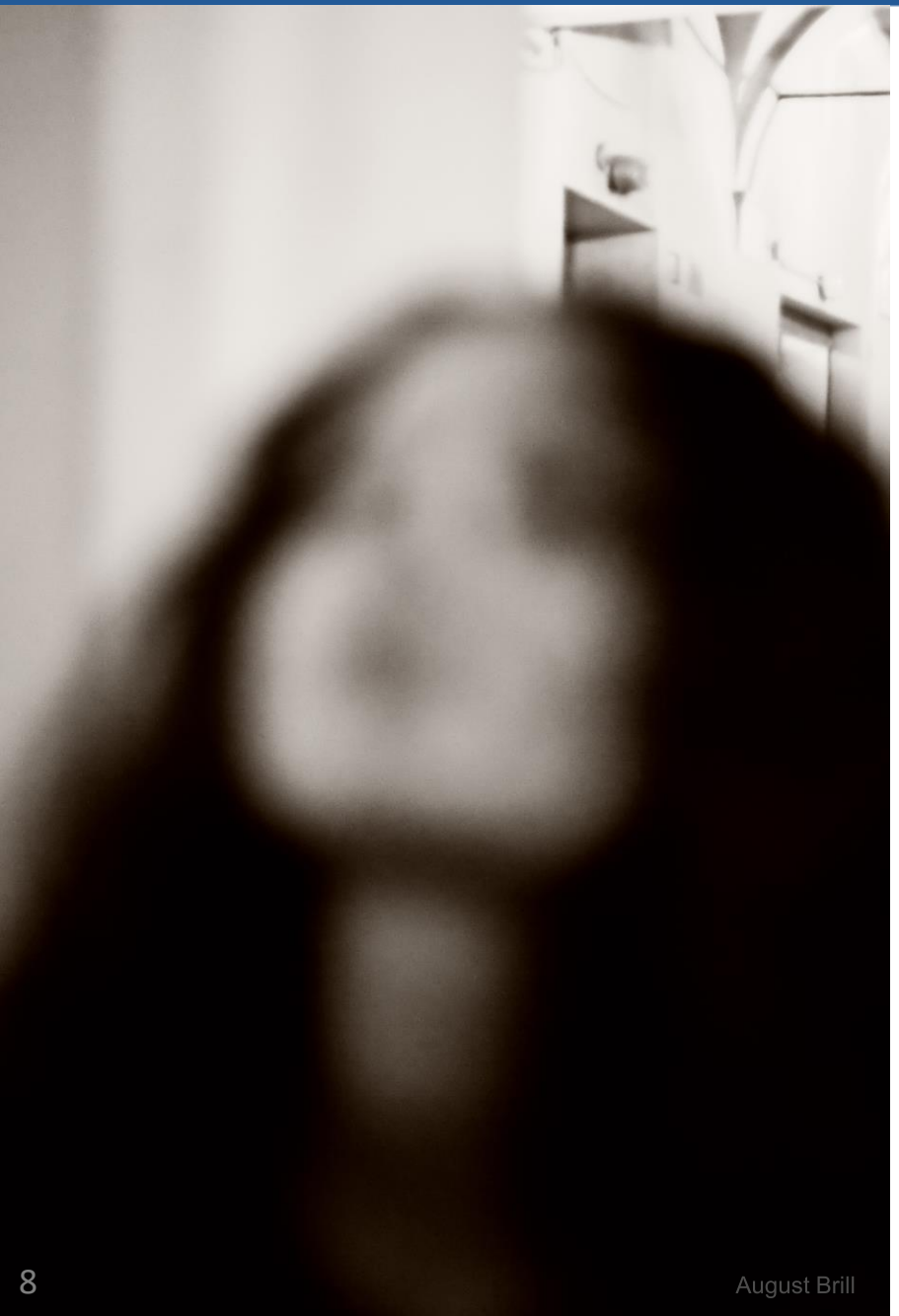
Advanced cryptography



Potential within government context

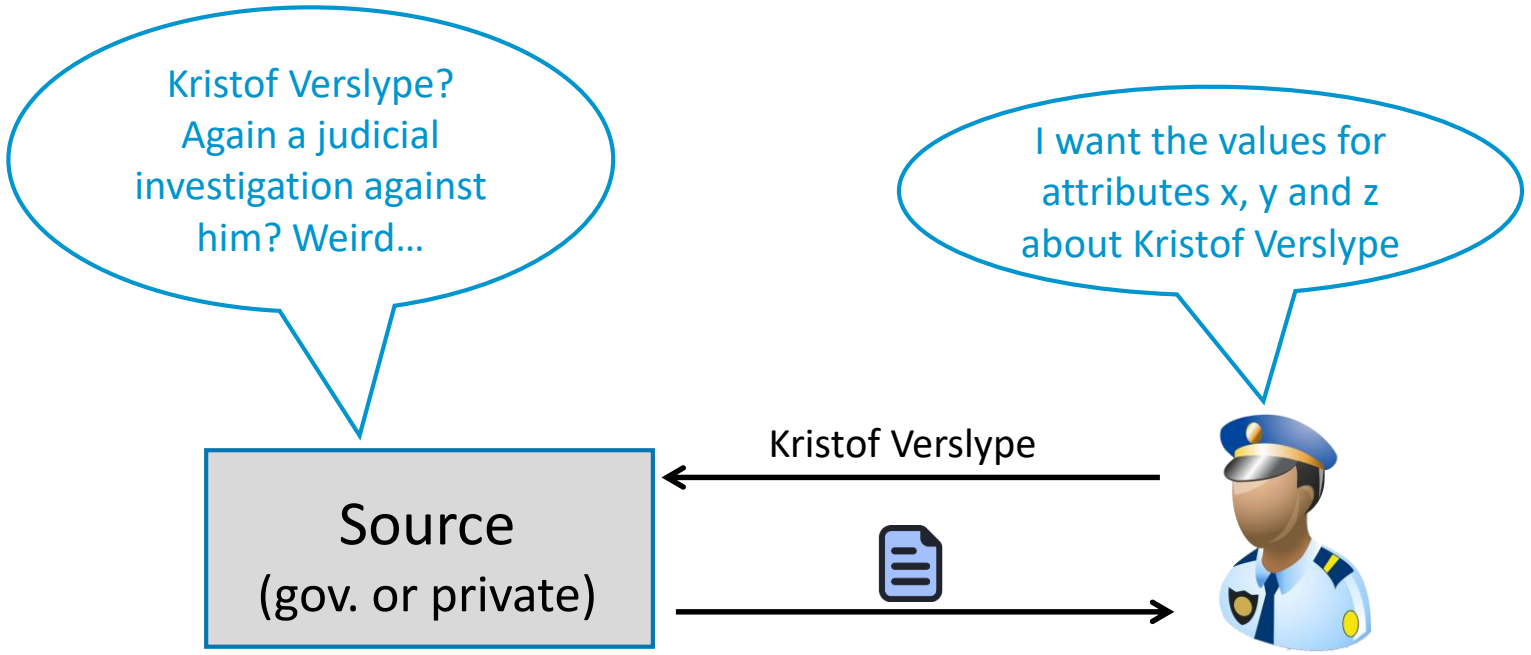
Oblivious transfer

Oblivious transfer – Problem statement



Scenario

Investigation by Ministery of Justice of into specific citizen
Ministery needs information provided by multiple sources

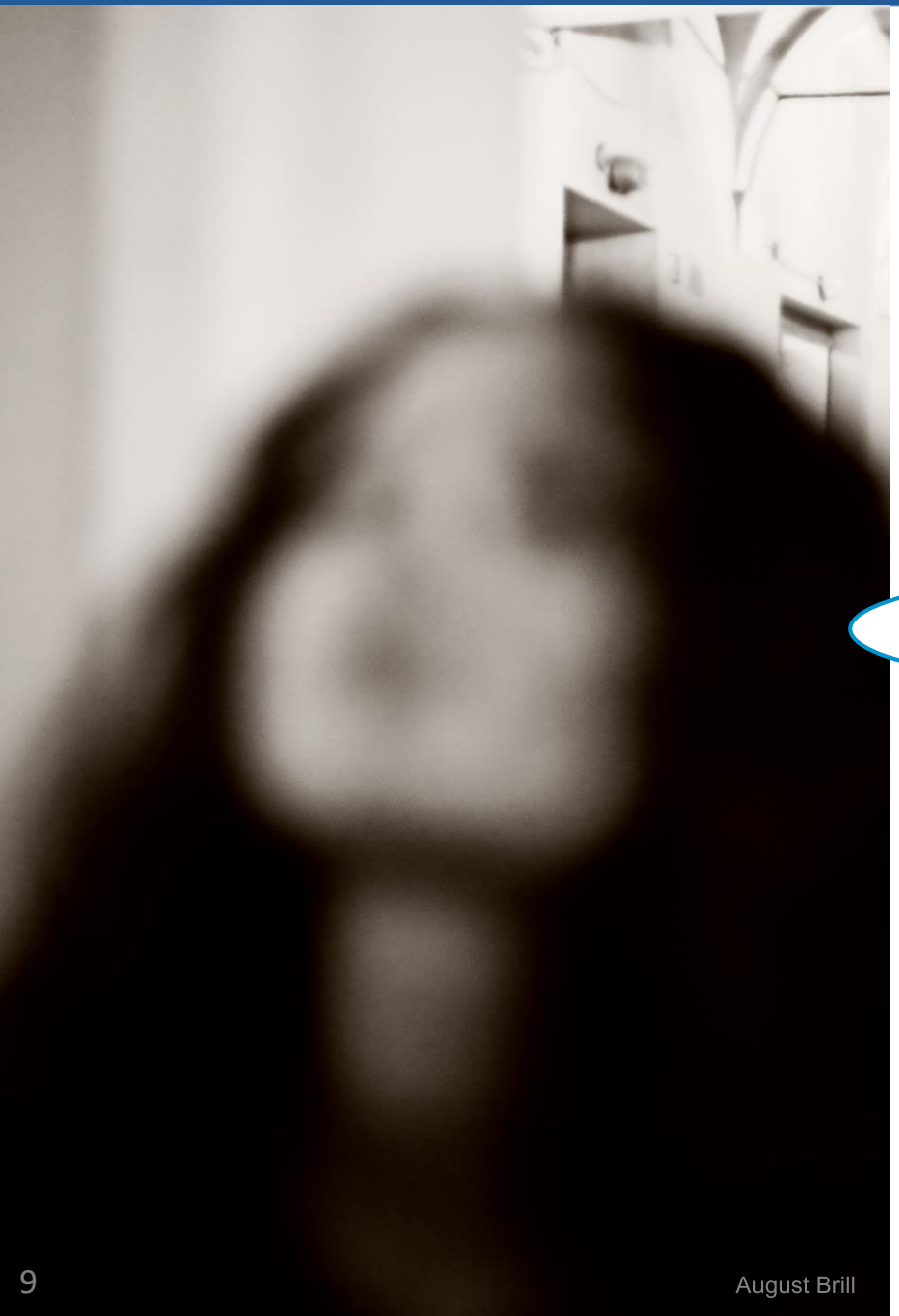


Proportionality
Privacy subject towards source
Confidentiality of investigation

Smals ICT for society

August Brill

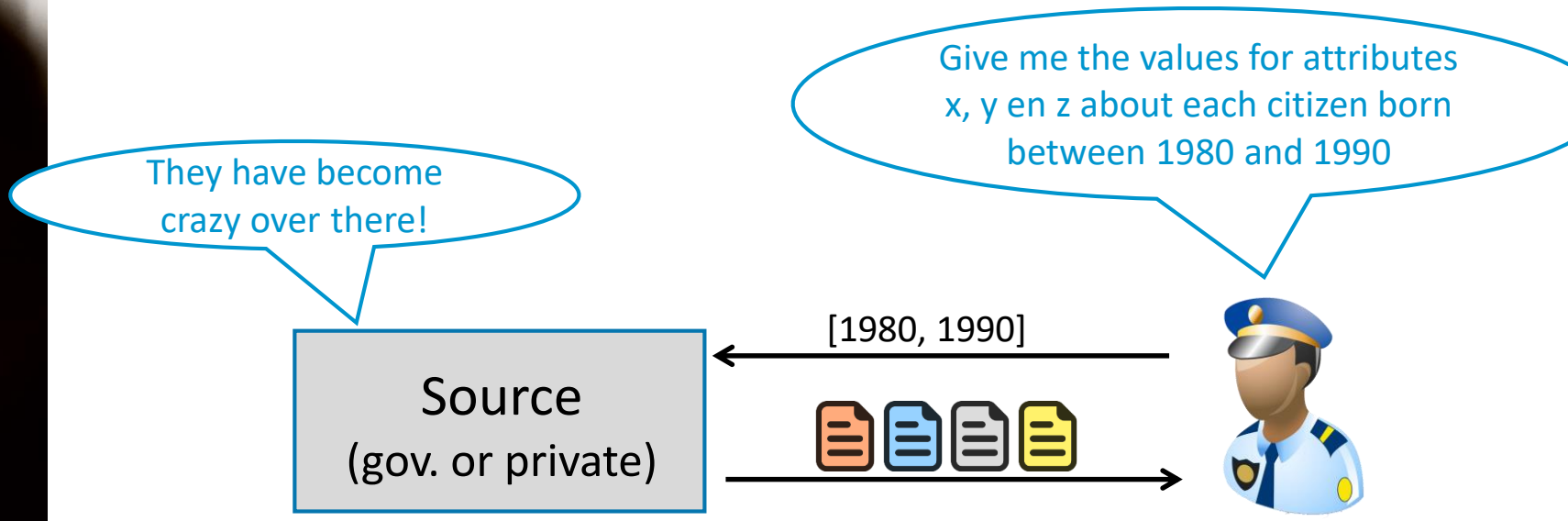
Oblivious transfer – Problem statement



Scenario

Investigation by Ministery of Justice against a specific citizen

Ministery needs information provided by multiple sources



Proportionality

Privacy subject towards source

Confidentiality of investigation

Smals ICT for society

Oblivious transfer - Tension

Privacy of citizen & confidentiality investigation towards sources

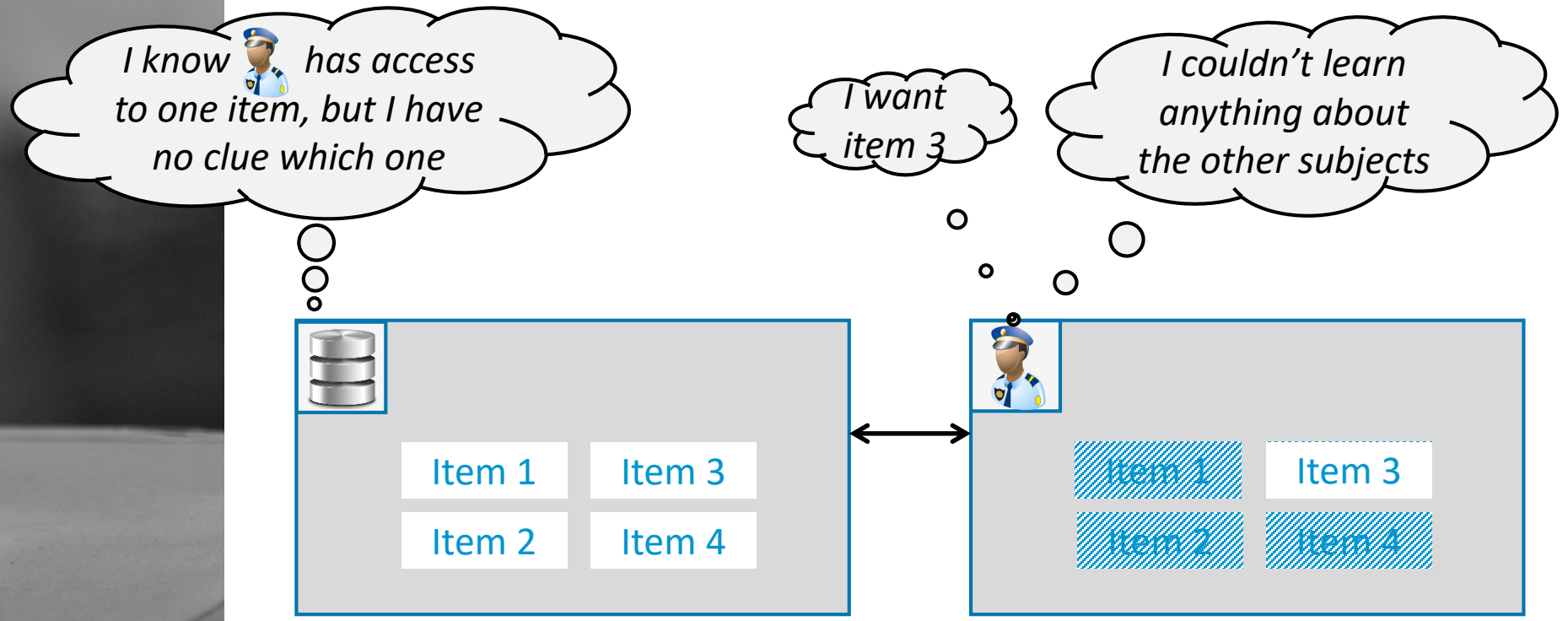
Tension

Proportional processing of personal data by ministery of justice

Jobeca (Jarr1520) @ Flickr

Oblivious transfer - Concept

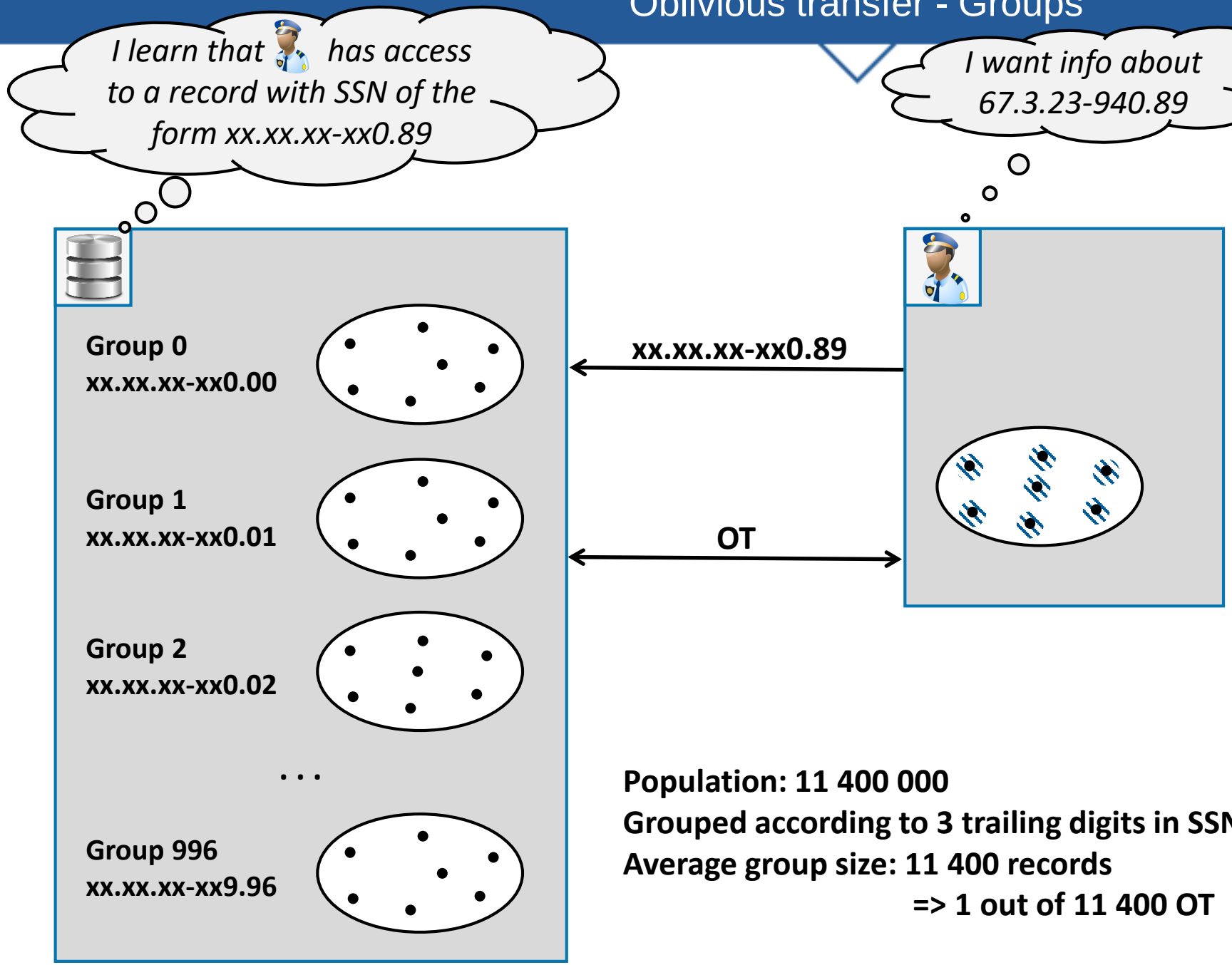
Te sender provides to a receiver access to one item out of a bigger set of items. De sender does not learn which item.



Sologenesis (Leo) @ Flickr

Smals ICT for society

Oblivious transfer - Groups

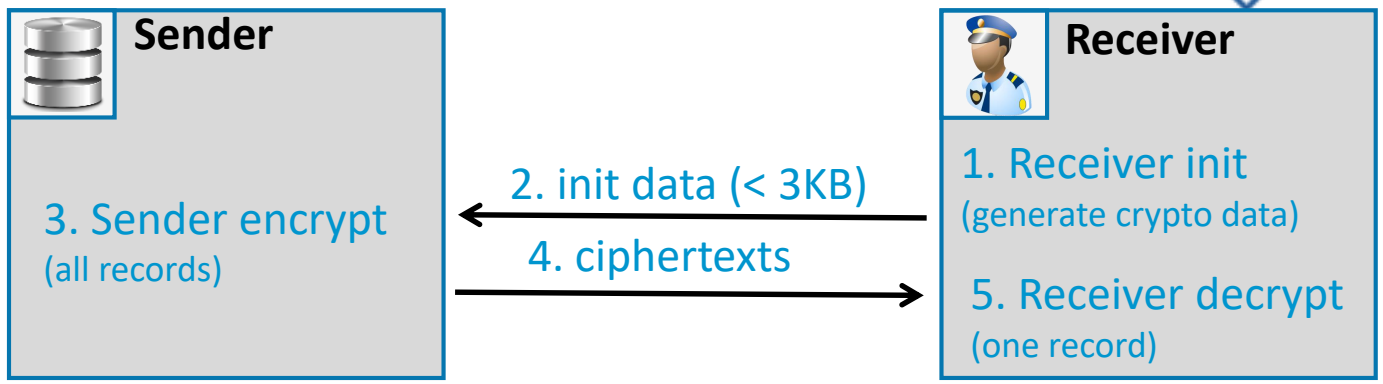


Population: 11 400 000
Grouped according to 3 trailing digits in SSN
Average group size: 11 400 records
=> 1 out of 11 400 OT

In reality

- Millions of records, but grouped. OT applied on one group
- Legal obligation to remove irrelevant ciphertexts asap

Oblivious transfer – Implementation & performance



Computational load at sender

256 bit security, standard laptop

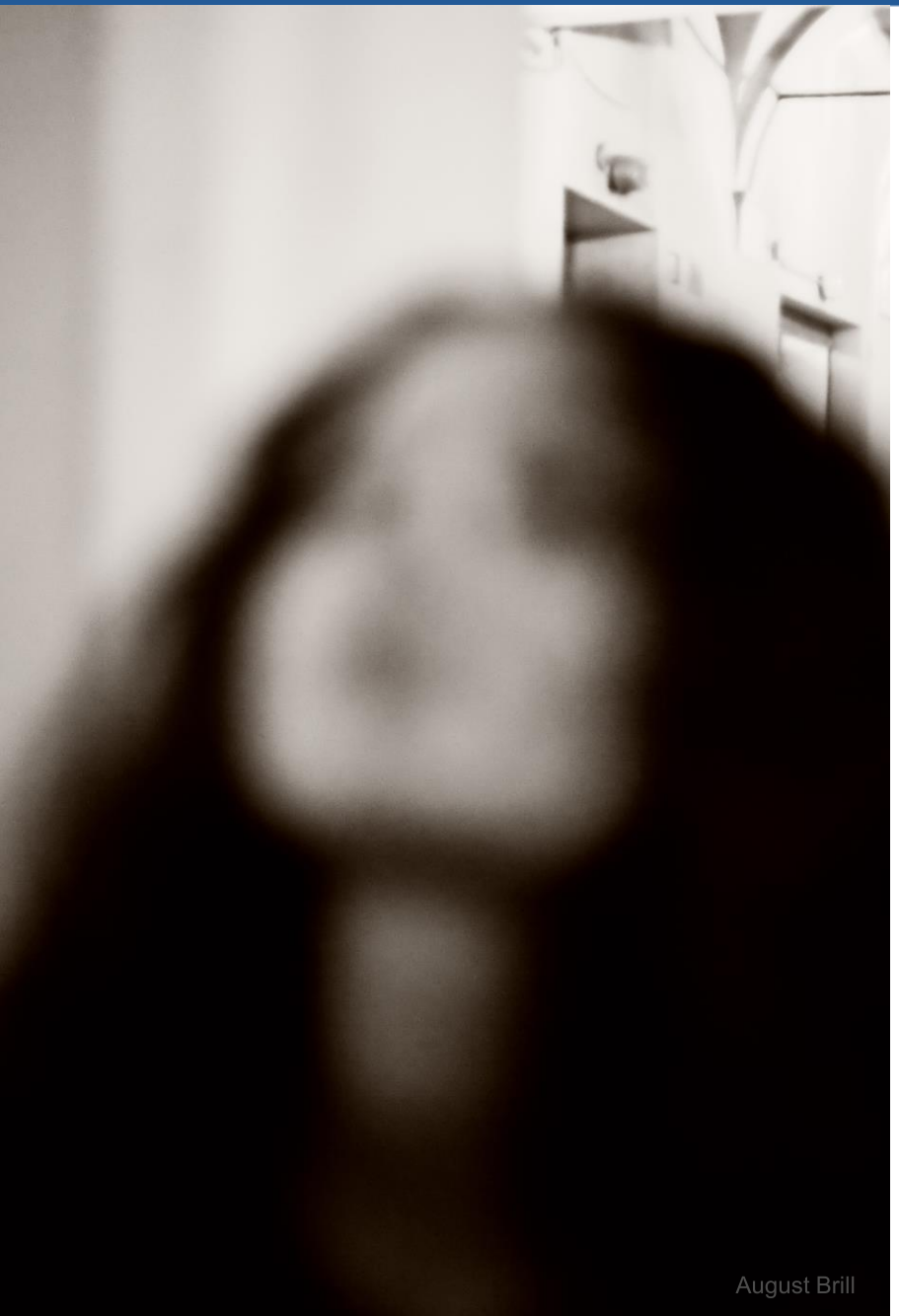
	1 out of 1000 records			1 out of 10 000 records			1 out of 25 000 records		
	Receiver init O(log n)	Sender encrypt O(log n*s)	Receiver decrypt O(s + log n)	Receiver init O(log n)	Sender encrypt O(log n*s)	Receiver decrypt O(s + log n)	Receiver init O(log n)	Sender encrypt O(log n*s)	Receiver decrypt O(s + log n)
20,7KB/rec.	213ms	925ms	30ms	299ms	4896ms	27ms	289ms	11544ms	37ms
103,4KB/rec	214ms	2604ms	33ms	270ms	22 146ms	36ms	282ms	54586ms	40ms

Setup
Data in-memory / Lenovo Thinkpad L570, Windows 10, Intel Core i5-6300 CPU @ 2,40Ghz, 16GB, P-521 curve, no multithreading.
Only of crypto calculations, not of storage I/O or communication
Average of 10 runs is taken

Smals Research Java implementation

- M Byali, A Patra, D Ravi, P Sarkar. *Fast and Universally-Composable Oblivious Transfer and Commitment Scheme with Adaptive Security*. IACR Cryptology ePrint Archive, **2017**
- C. Peikert, V. Vaikuntanathan, B. Waters. *A Framework for Efficient and Composable Oblivious Transfer.* CRYPTO 2008: Advances in Cryptology – **CRYPTO 2008** pp 554-571

Oblivious transfer



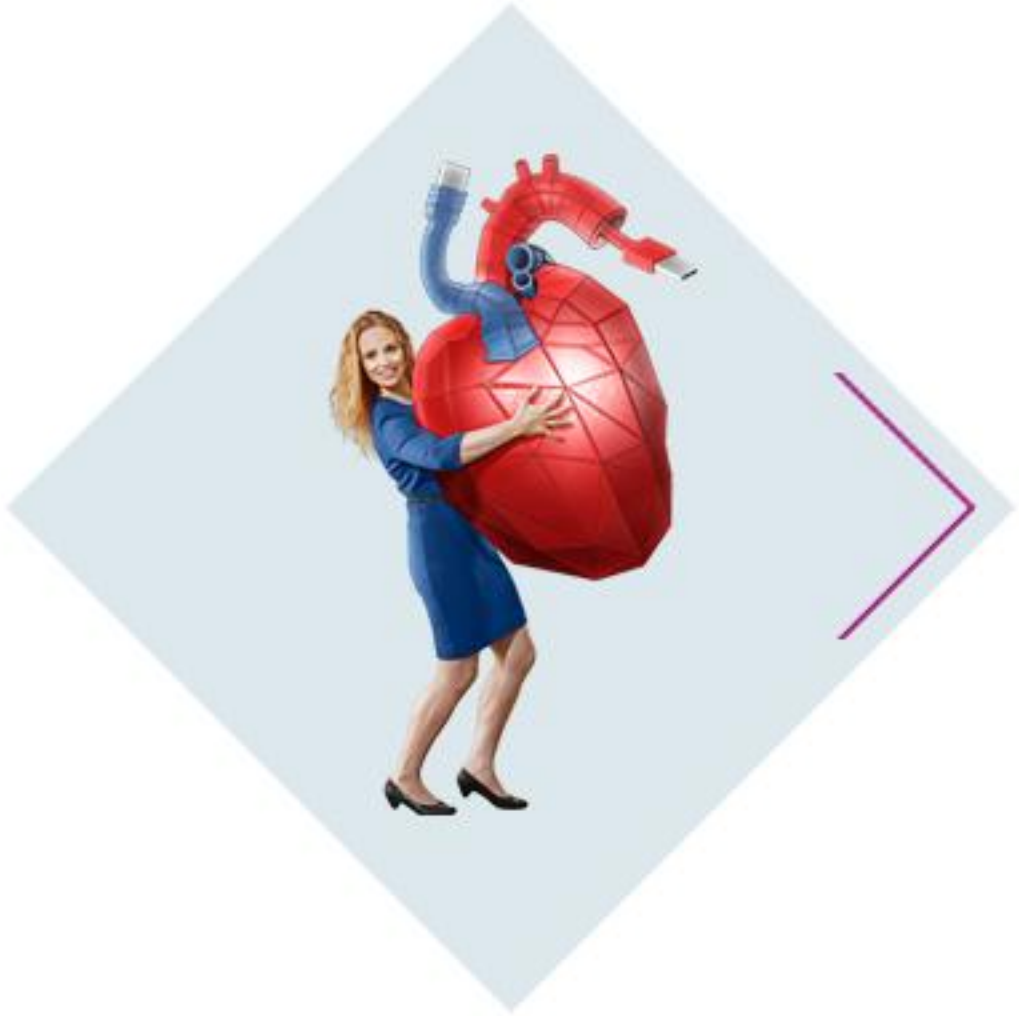
Concept

- Active research domain with advanced protocols
- High efficiency
- Own Java implementation

Applicability

- Answer to a concrete need
- New technology for our sector
- Will take while to get it in production

Smals
ICT for society



Oblivious join

Concept by Smals Research

Fictional example

Citizen selection

- All persons self-employed as secondary activity
- With a wage above € 50 000 / year as employee

Required data

- Specific medical data &
- Data about insurance as independent

Cooperation by multiple organisations required

RSZ - ONSS - LSS

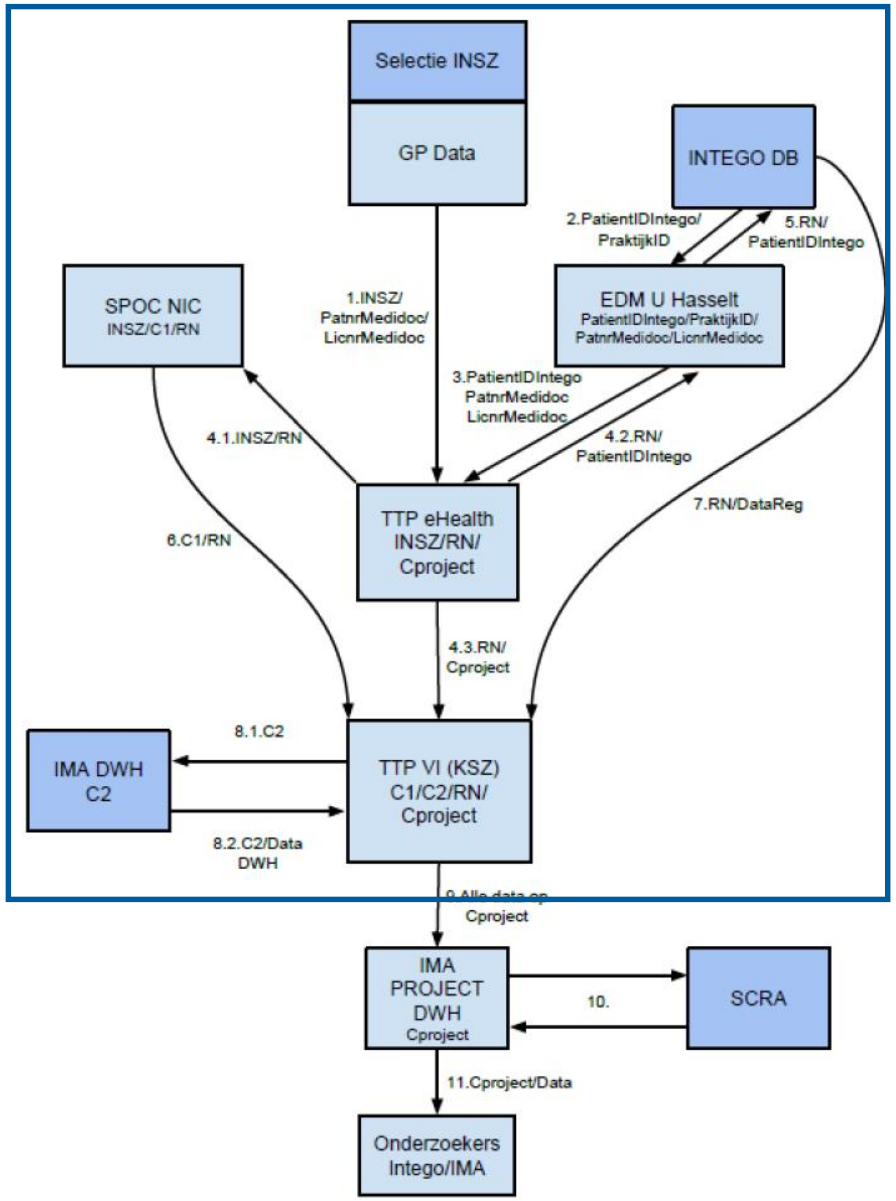
RSVZ

Belgian Cancer Registry

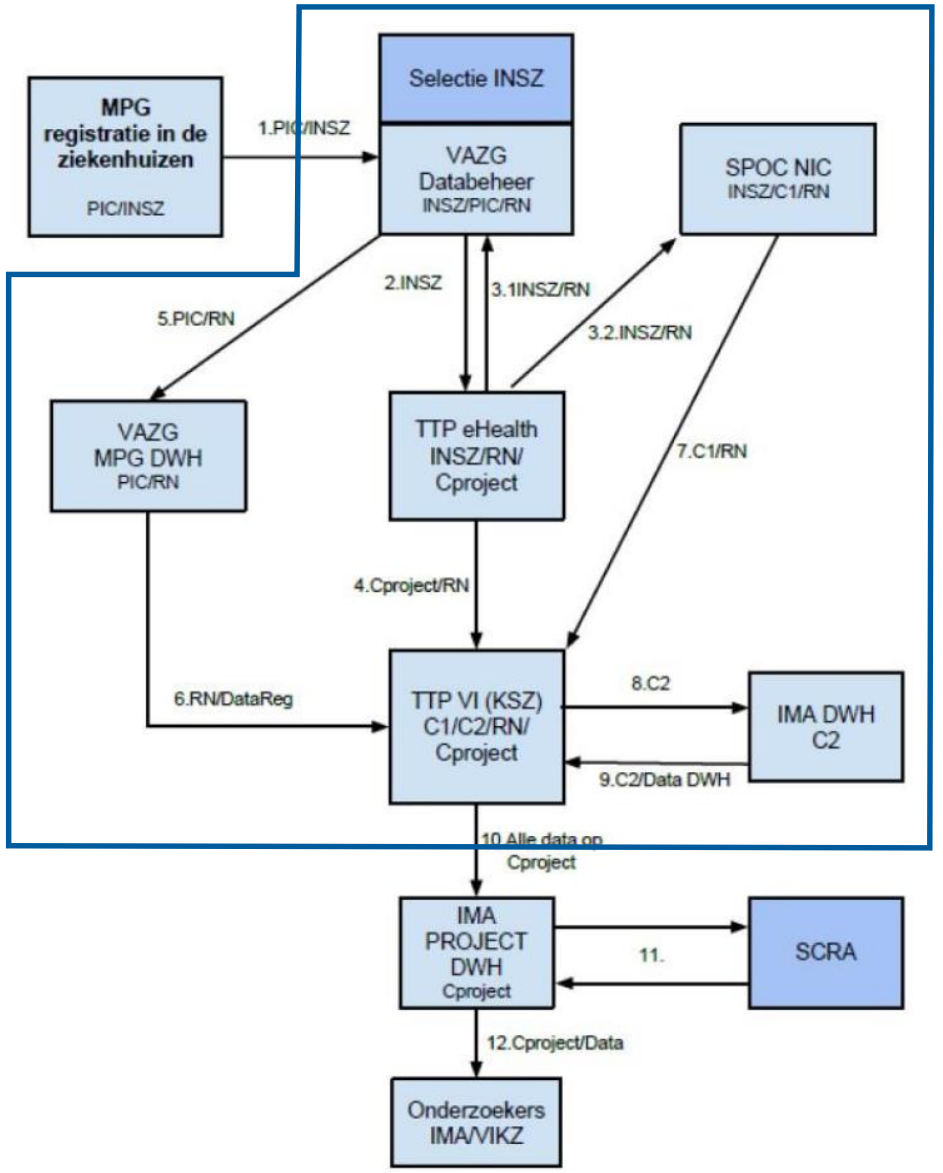
Joining and pseudonymizing personal data from multiple sources for research purposes

Joining personal data – Current practice

Example 1



Example 2



KSZ BCSS

Deliberation nb. 17/071 from 19/9/17 (left)

Deliberation nb. 19/062 from 2/4/19 (right)

- Complex flow
- Bespoke
- Slow
- Security risks
- Data leakage

Oblivious join – Data leakage

Context

Joining and pseudonymizing personal data from multiple sources for research purposes

Scenario

Citizen selection

- All persons self-employed as secondary activity
- With a wage above € 50 000 / year as employee

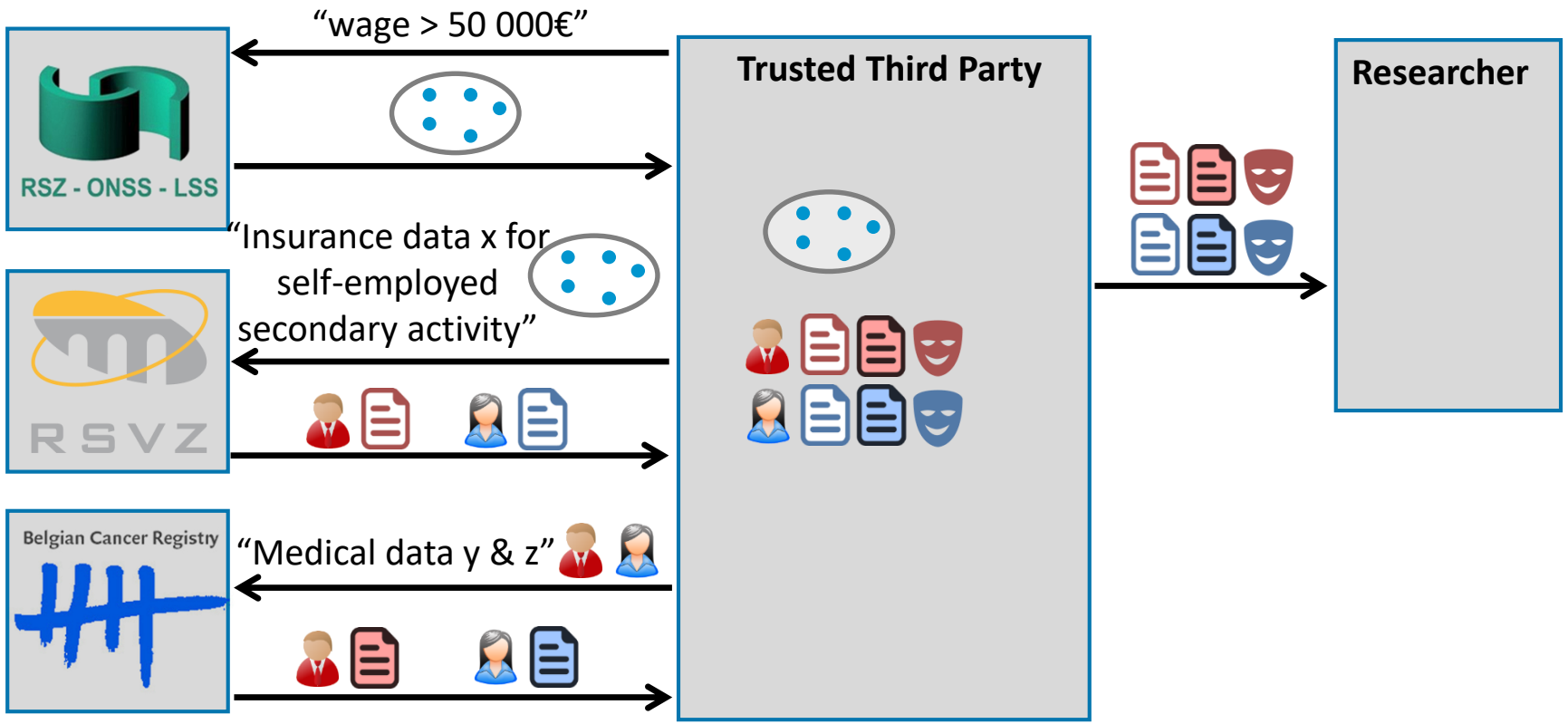
Required data

- Specific medical data
- Data about insurance as independent

Issues

- Data leakage towards senders and/or TTP
- Extra intermediaries increase complexity

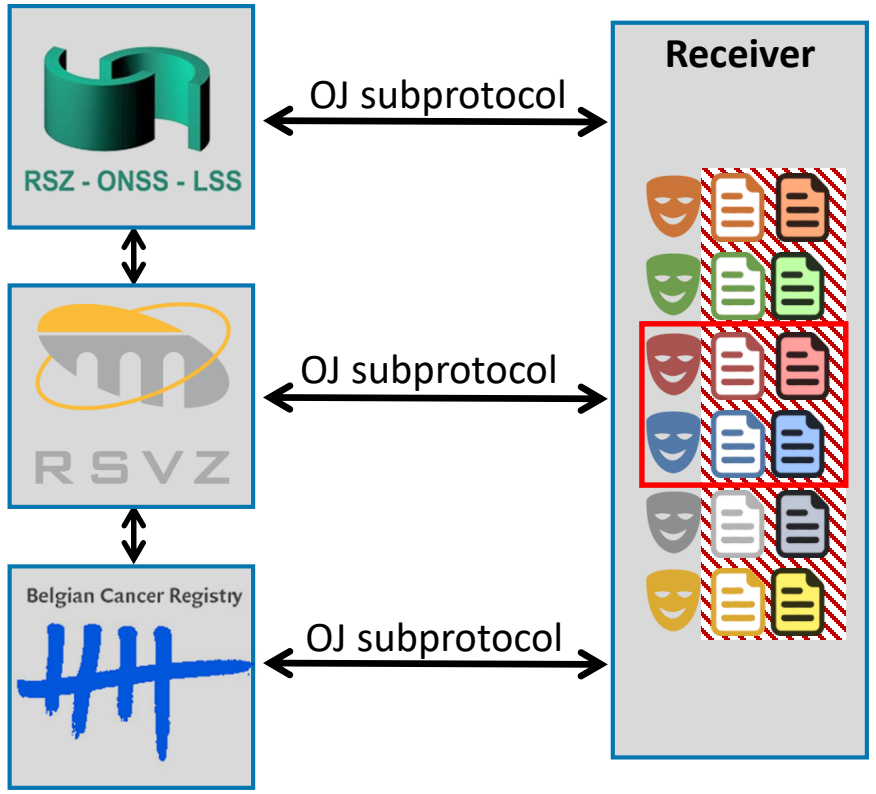
Potential traditional approach



Oblivious join

Idea

- Each sender sends all potentially relevant data to the receiver, but encrypted and pseudonymized
- Receiver can decrypt iff something received about the same citizen from each sender



Senders don't learn (statistical or personal) data.

Receiver learns only required pseudonymized **personal** data.

Minimal leakage of **statistical data** leaks to the receiver

in example:

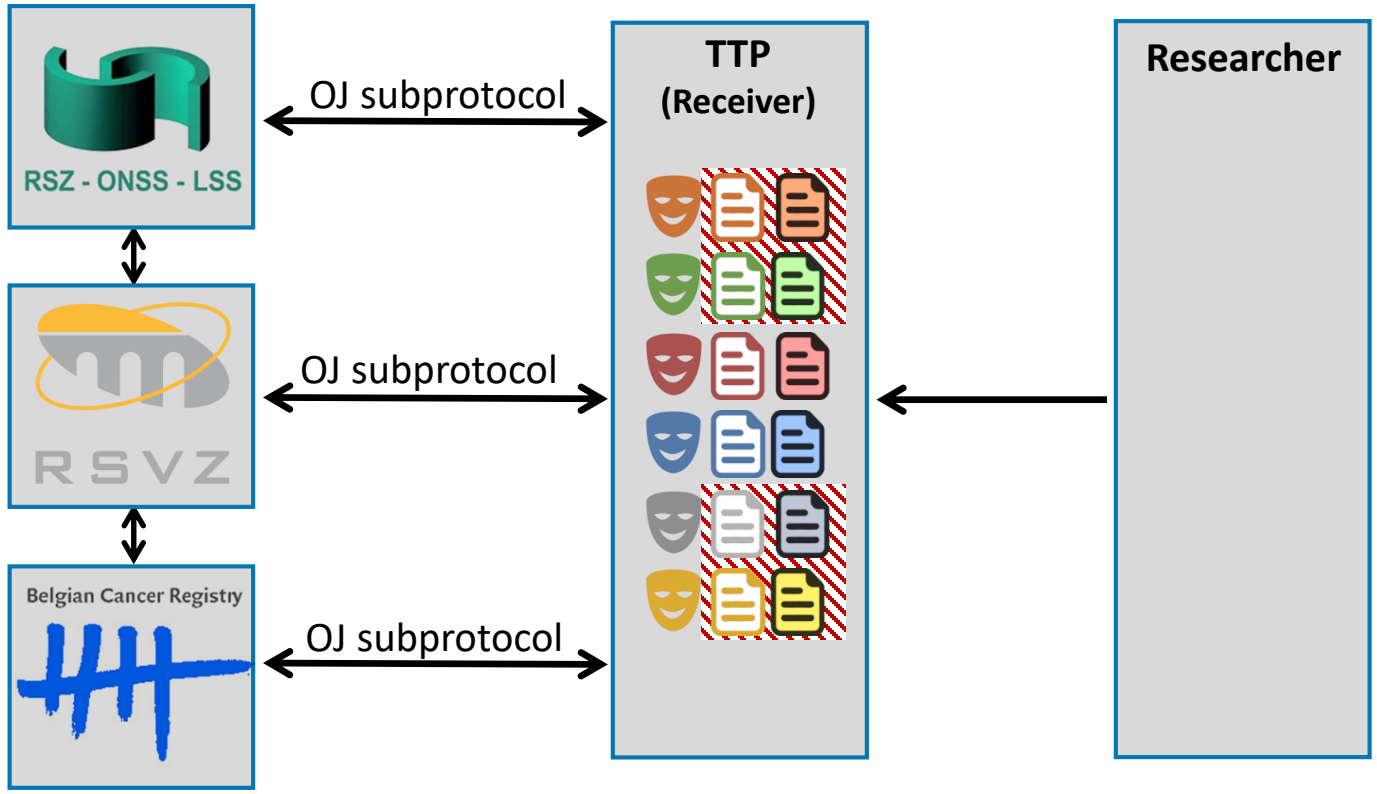
- #citizens with wage > € 50 000
- #independents as secondary activity

Smals ICT for society

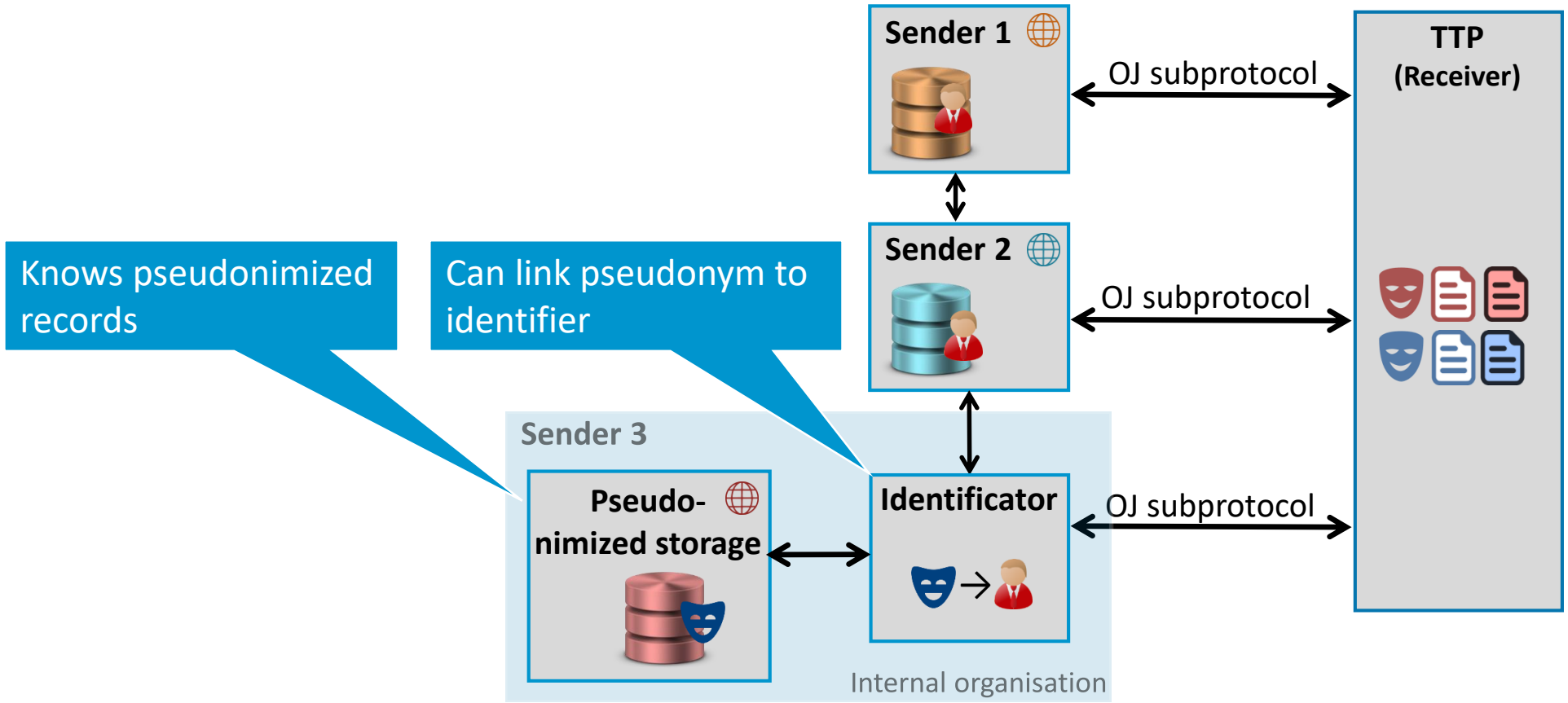
Oblivious join

TTP (Trusted third party)

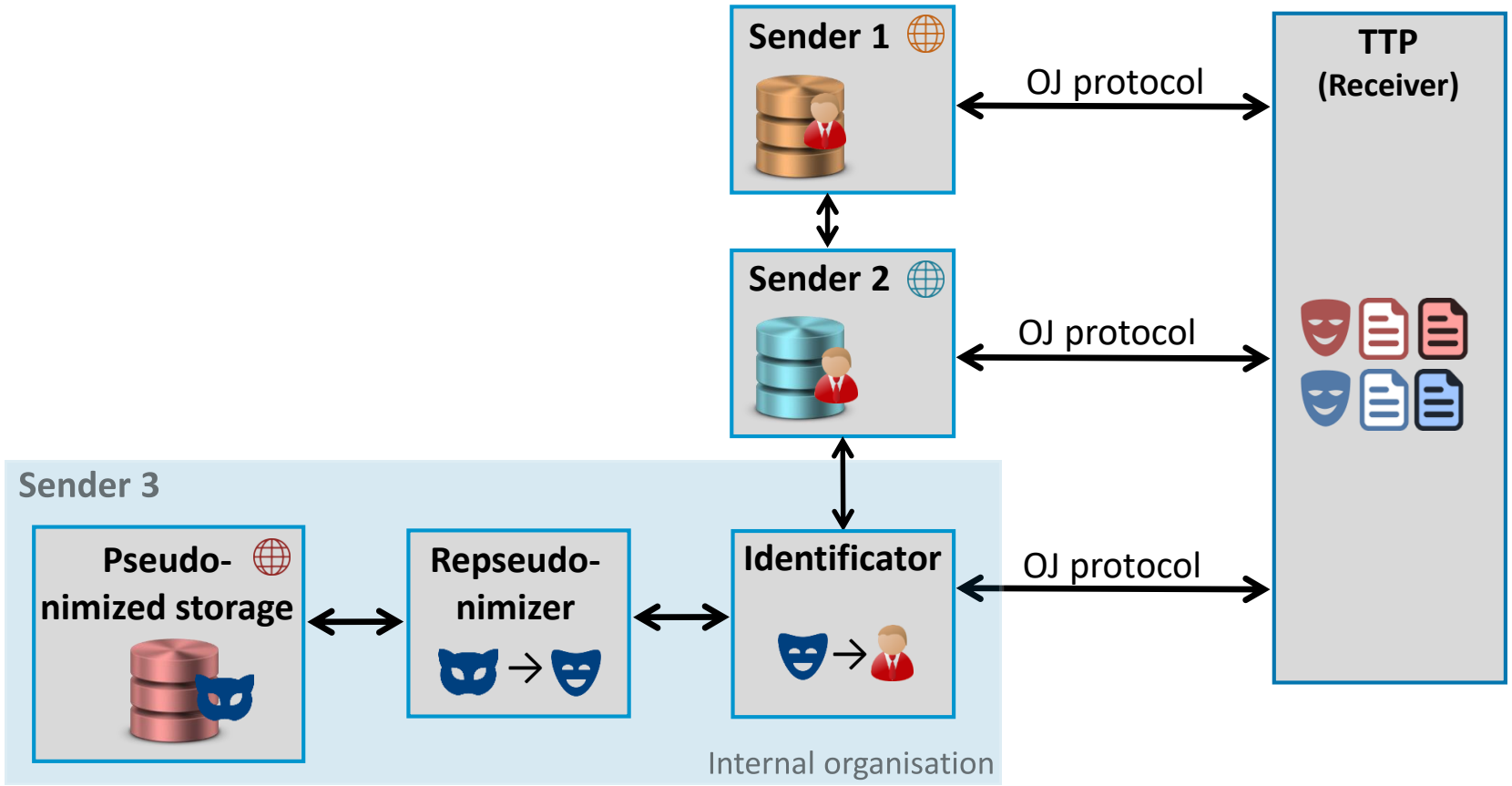
- Removes asap irrelevant ciphertexts
- Potentially does additional operations (e.g. checks)
- Access control w.r.t. researcher
- ‘Trust’ very limited



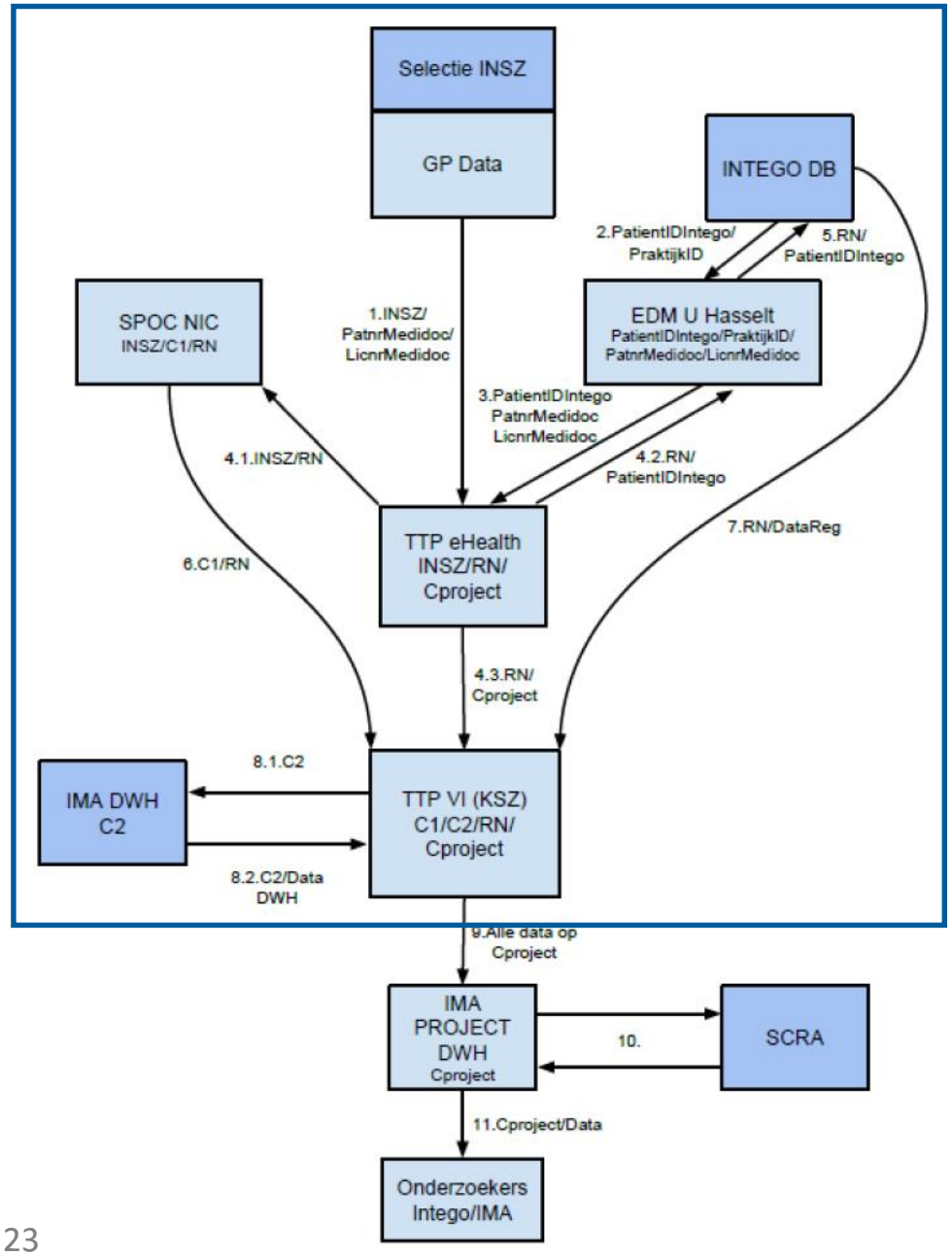
Oblivious join

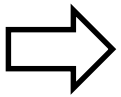


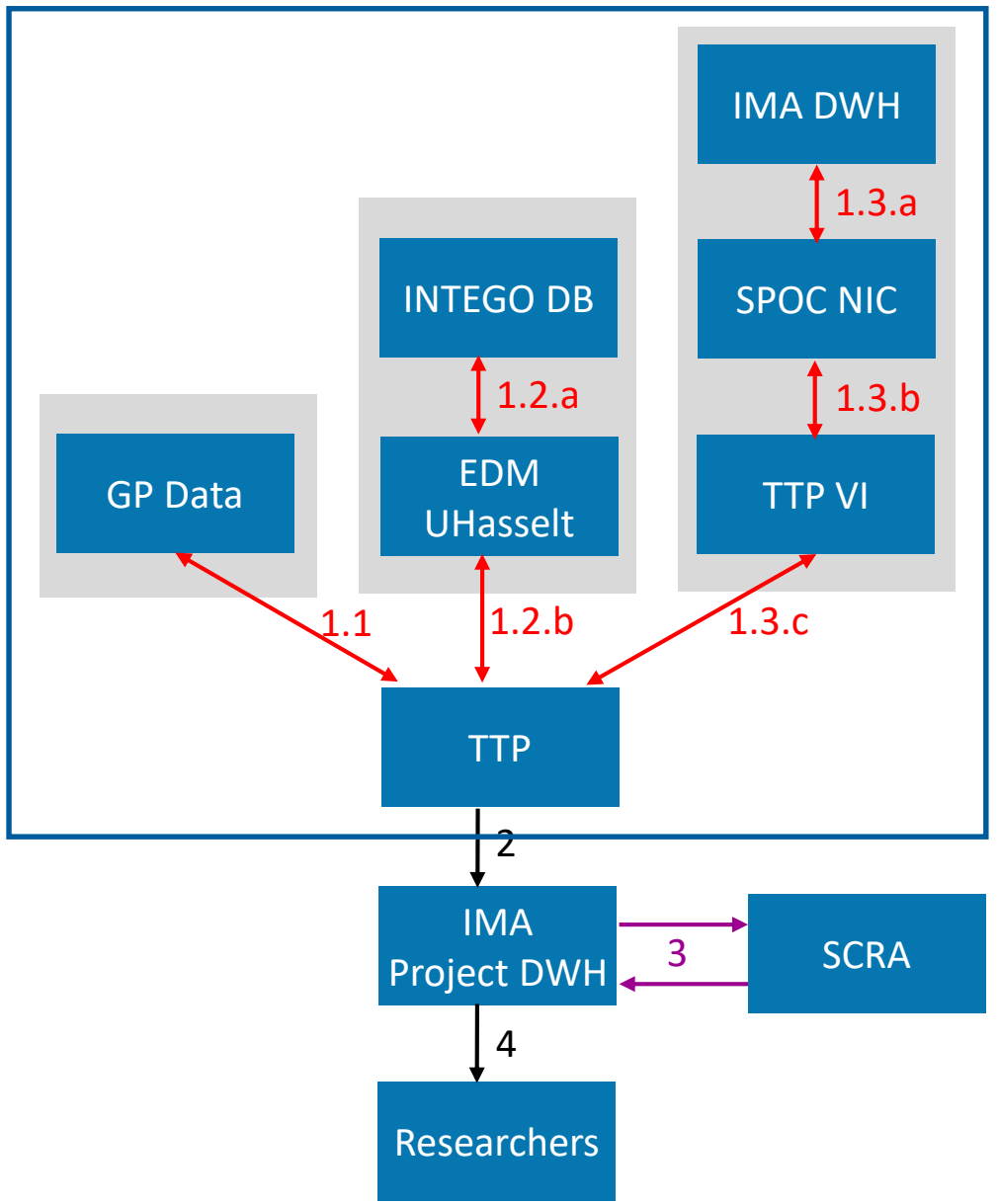
Oblivious join



Current practice Vs. Oblivious join







Deliberation nb. 17/071 from 19 September 2017

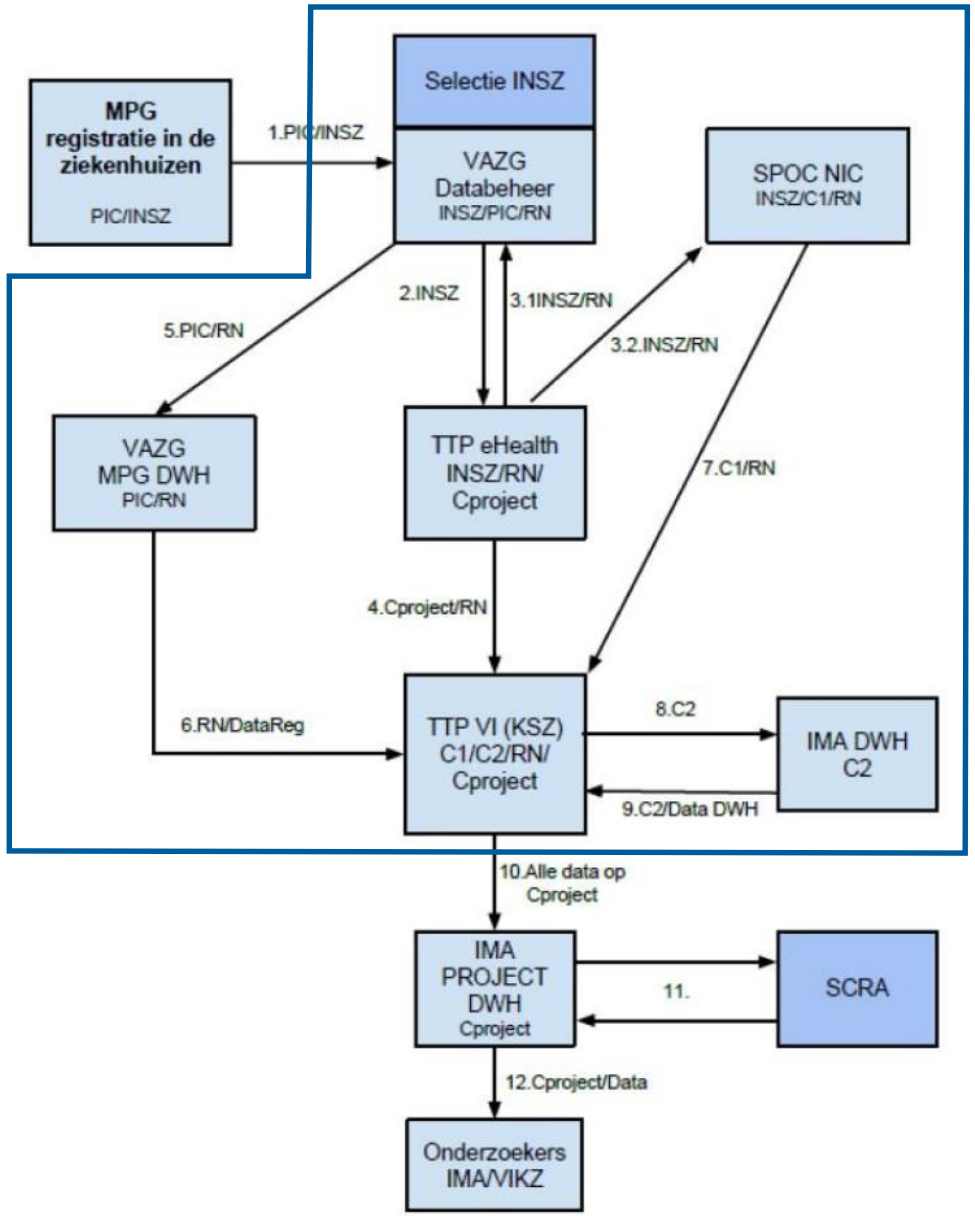
Oblivious join automated

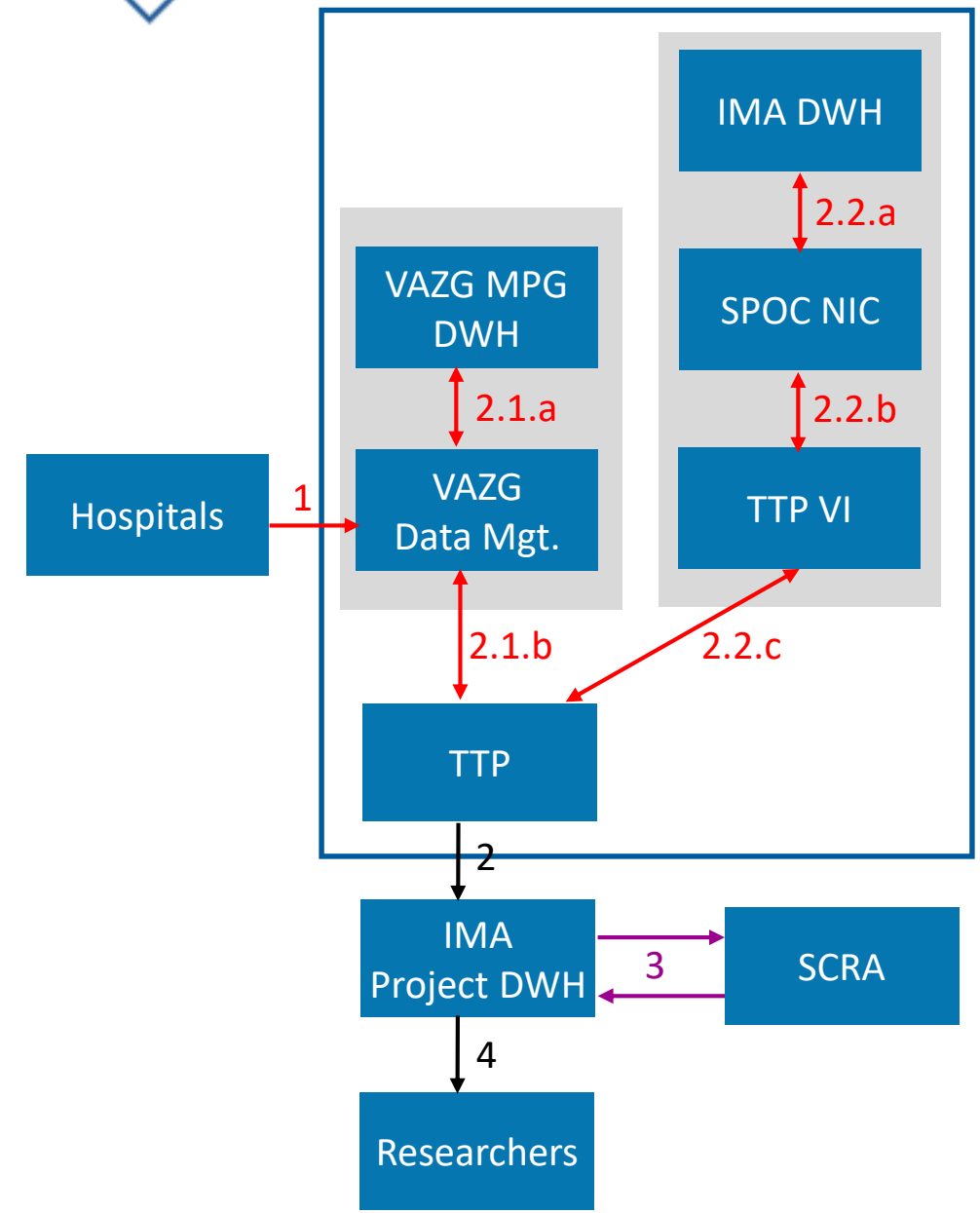
Analysis

Data transfer

Standard flow in parallel
No data leakage

Current practice Vs. Oblivious join





Deliberation nr. 19/062 from 2 April 2019

Oblivious join automated

Analysis

Data transfer

Standard flow in parallel
No data leakage

Oblivious join

Status

- **First library for test and demo purposes**
  with core functionality
- Efficiency for 256 bit security: “A few hours” [1]
- Technical description in progress
- Collaboration with legal and security services

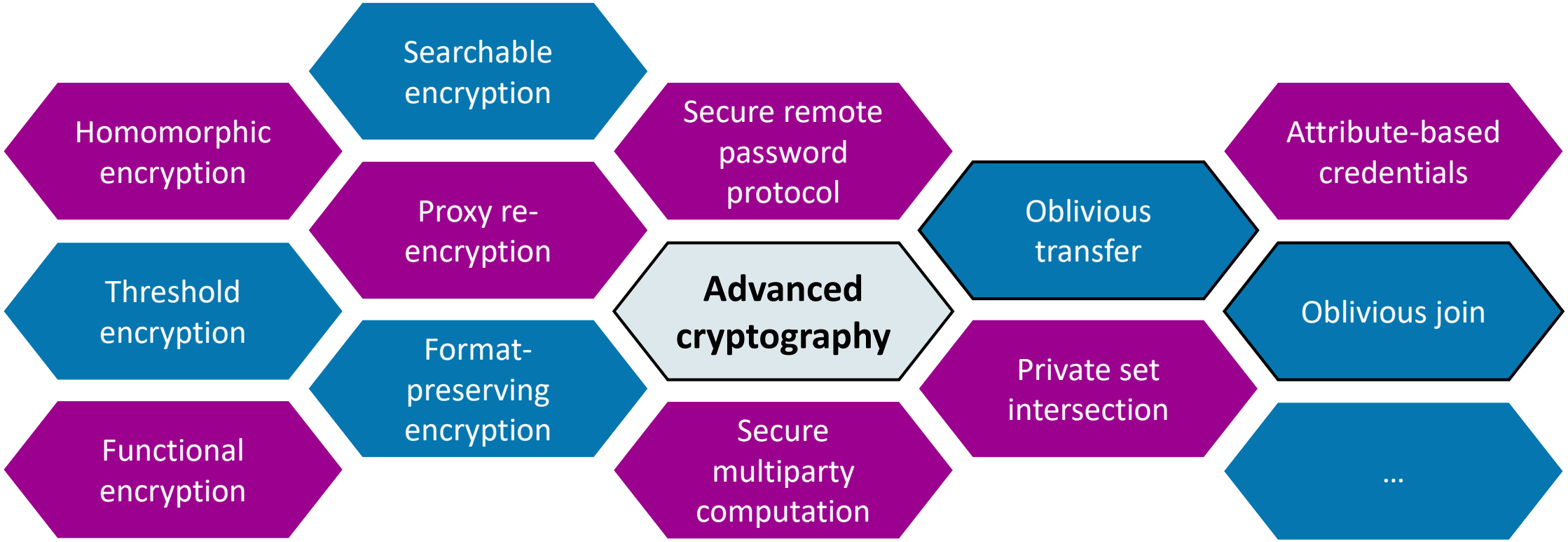
[1] Preliminary tests on Ubuntu 18.04, Intel Core i5-8250 CPU @ 1,60Ghz, 4 cores, 6GB

Joining & pseudonymizing personal data

- In a standardized way
- Without data leakage

Smals
ICT for society

Advanced cryptography



Potential within government context

Kristof Verslype
Cryptographer, PhD
Smals Research

Smals
ICT for society

Smals research sees opportunities within government context

Complex or hard to attain goals in a traditional way?

Functional requirements

Security & privacy (GDPR) requirements

Ongoing research

kristof.verslype@smals.be
+32(0)2 7875376
www.smals.be
www.smalsresearch.be
www.cryptov.net (personal)

Smals
ICT for society