Advanced cryptography for privacy protection

Cases from the government field

Kristof Verslype
PhD, Smals Research

20 dec. 2019

Smals
ICT for society

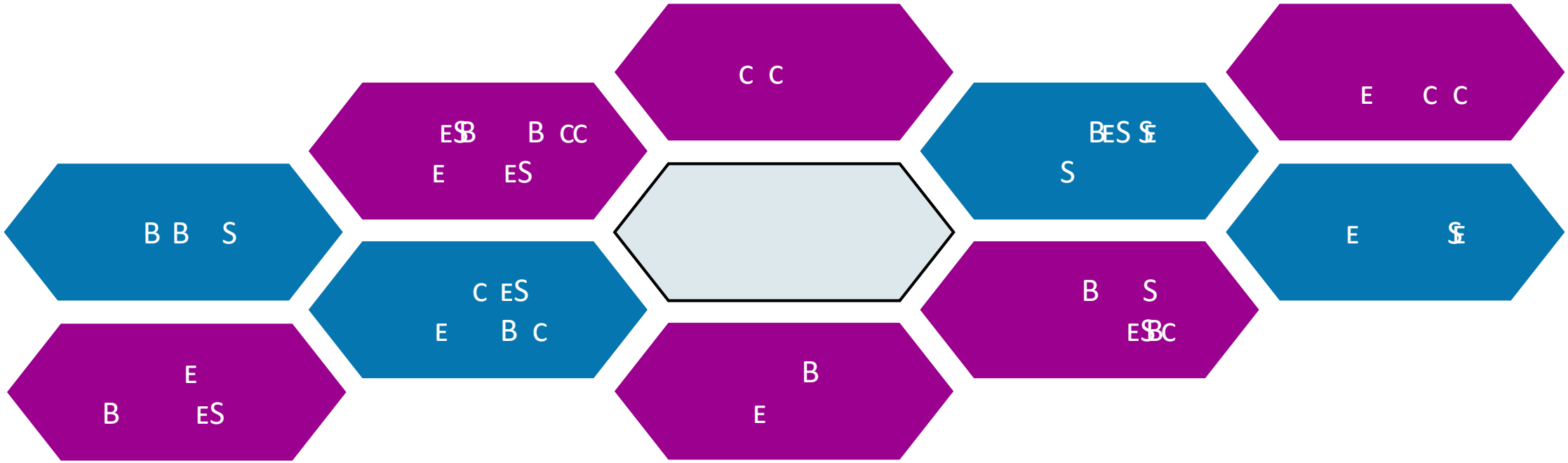
Smals
ICT for society

SUPPORT FOR E-GOVERNMENT

g-cloud

top EMPLOYER BELGIË BELGIQUE
CERTIFIED EXCELLENCE IN EMPLOYEE CONDITIONS

Smals Research



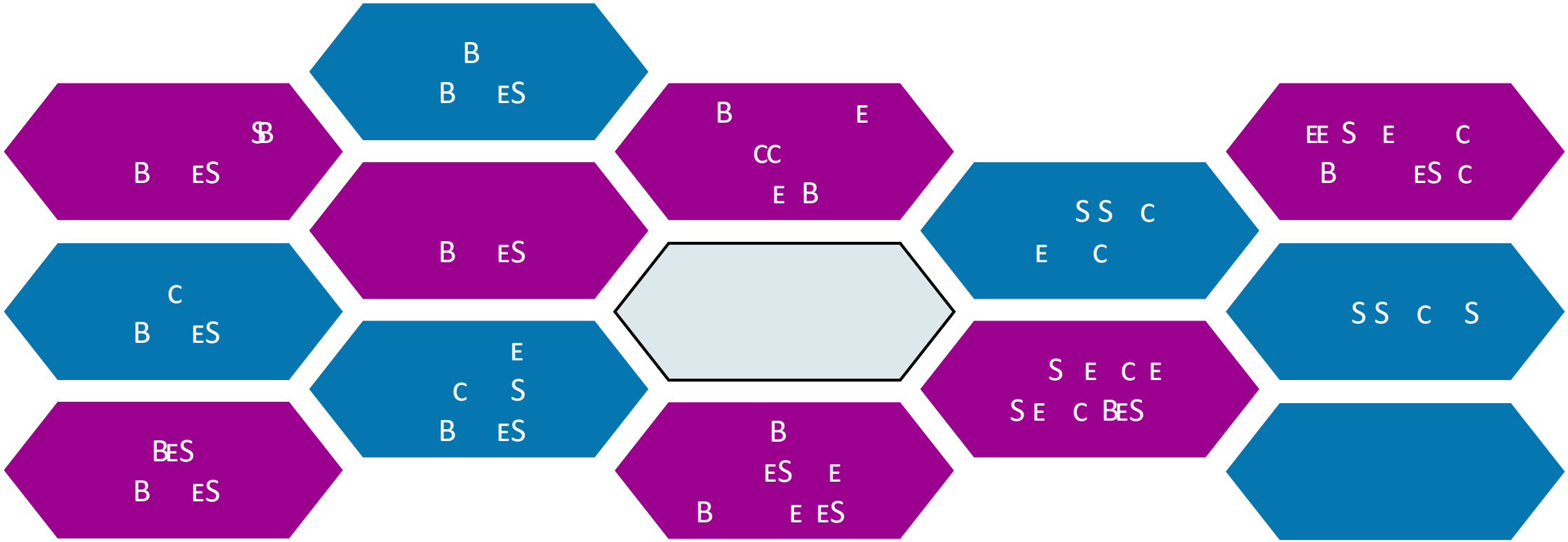
Smals
ICT for society

Modern cryptography

Much more is possible with cryptography

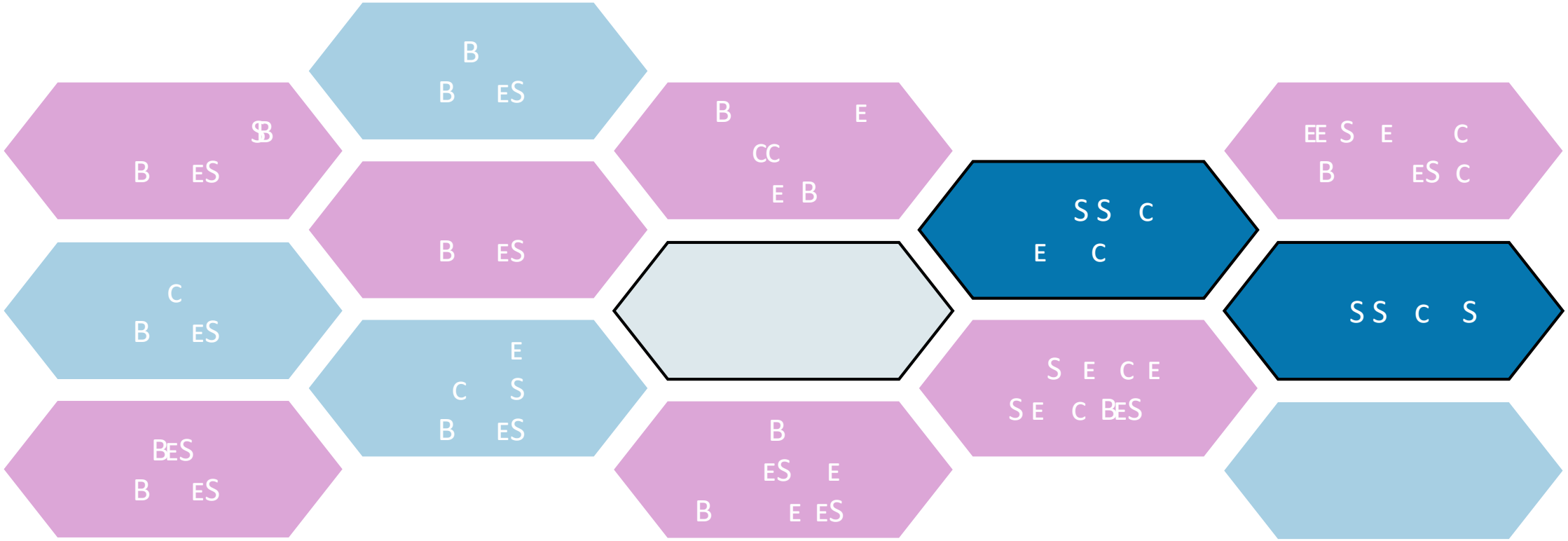
s

Advanced cryptography



Smals
ICT for society

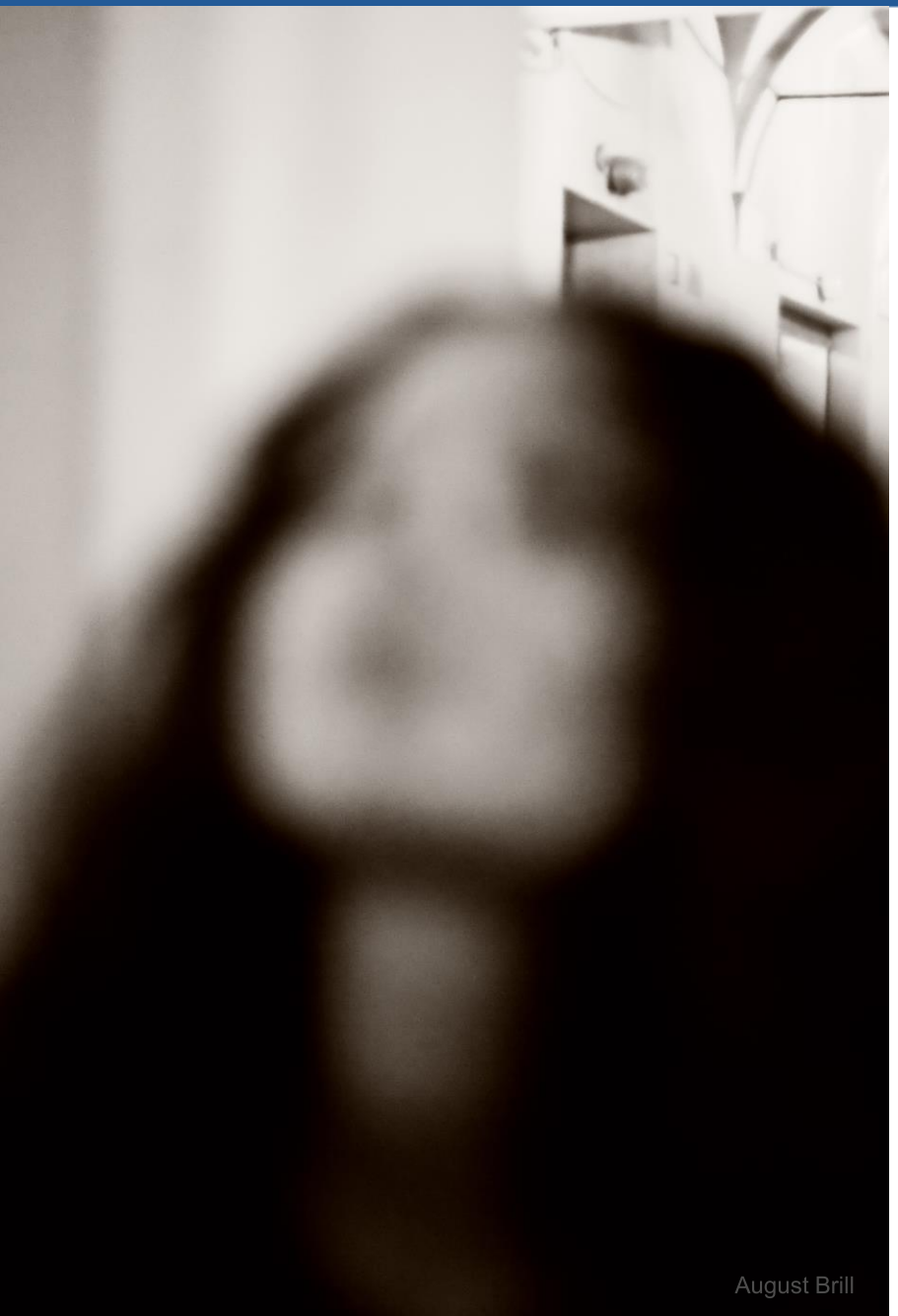
Advanced cryptography

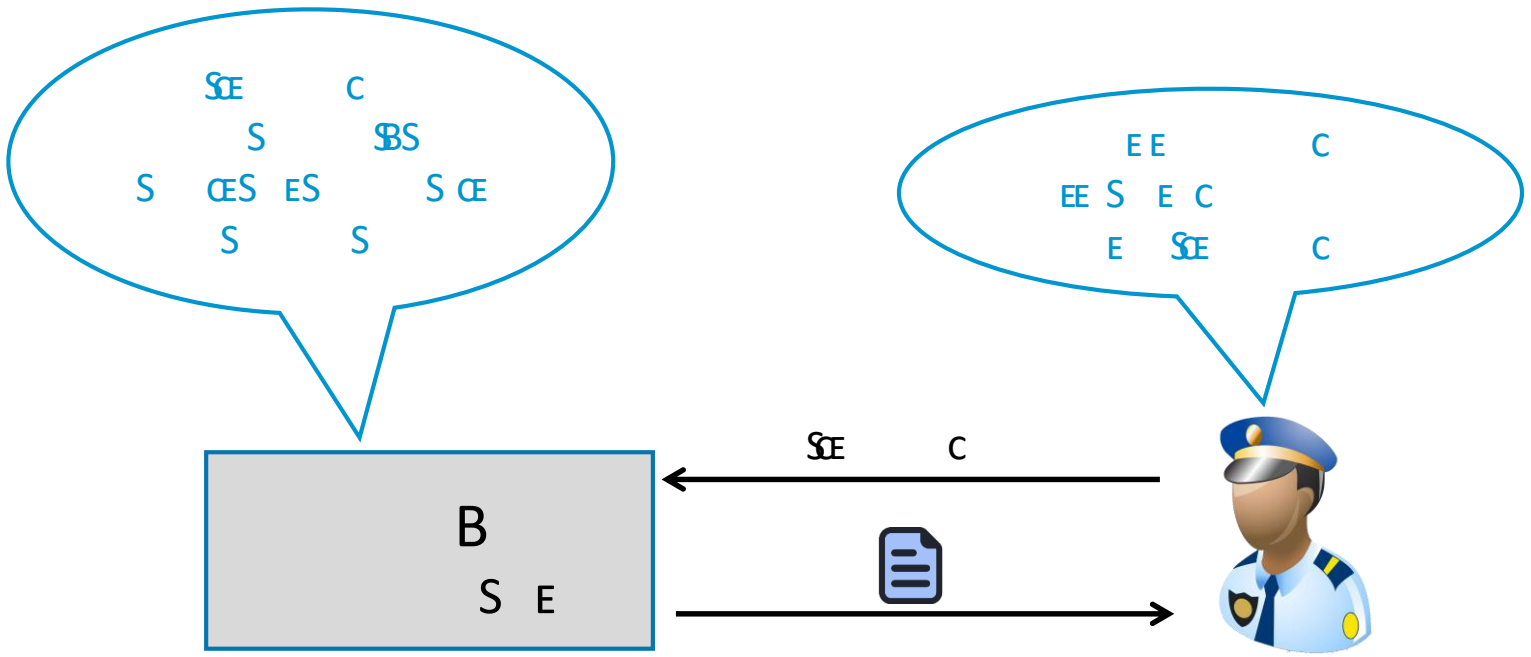


Smals
ICT for society

Oblivious transfer

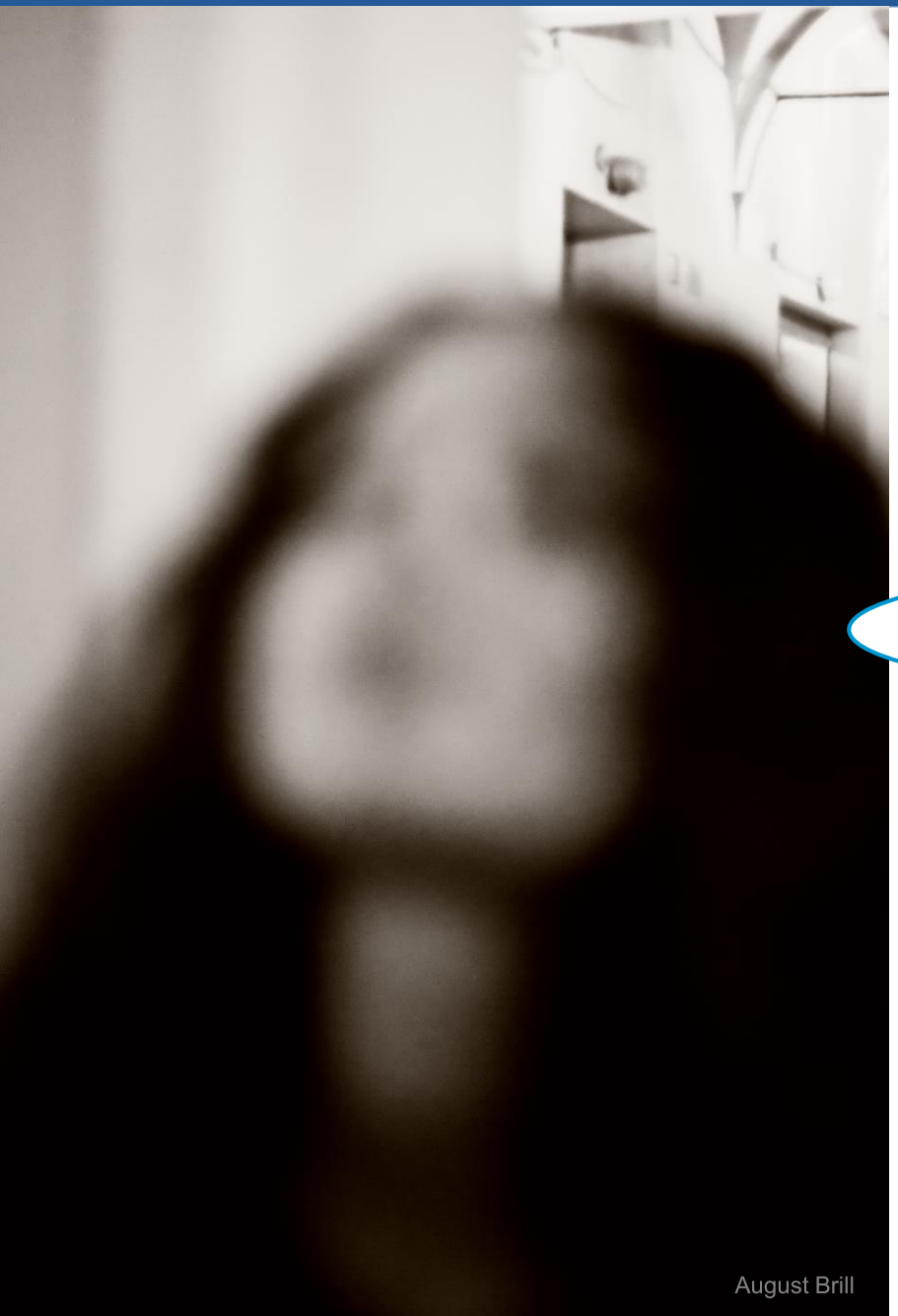
Oblivious transfer – Problem statement



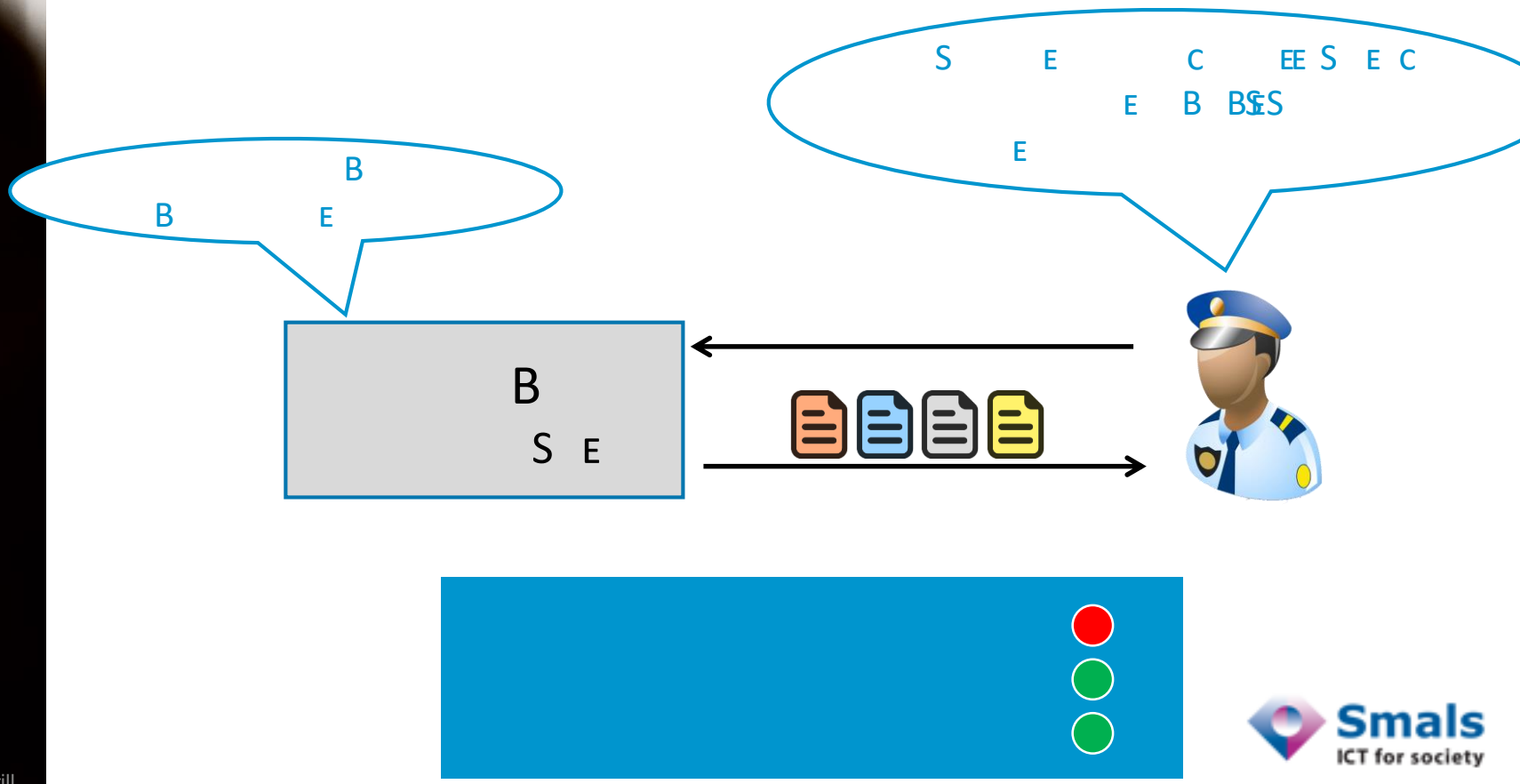


Smals
ICT for society

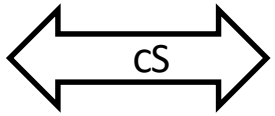
Oblivious transfer – Problem statement



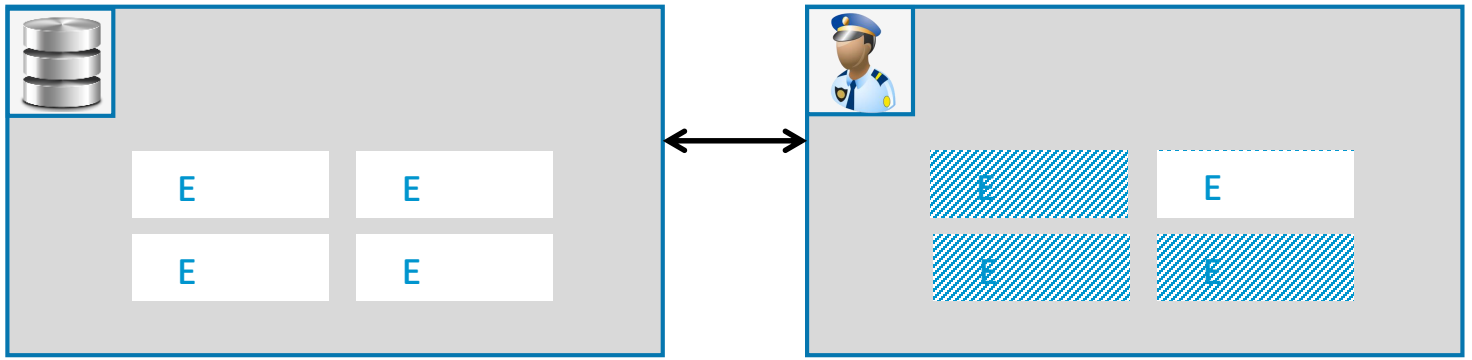
August Brill



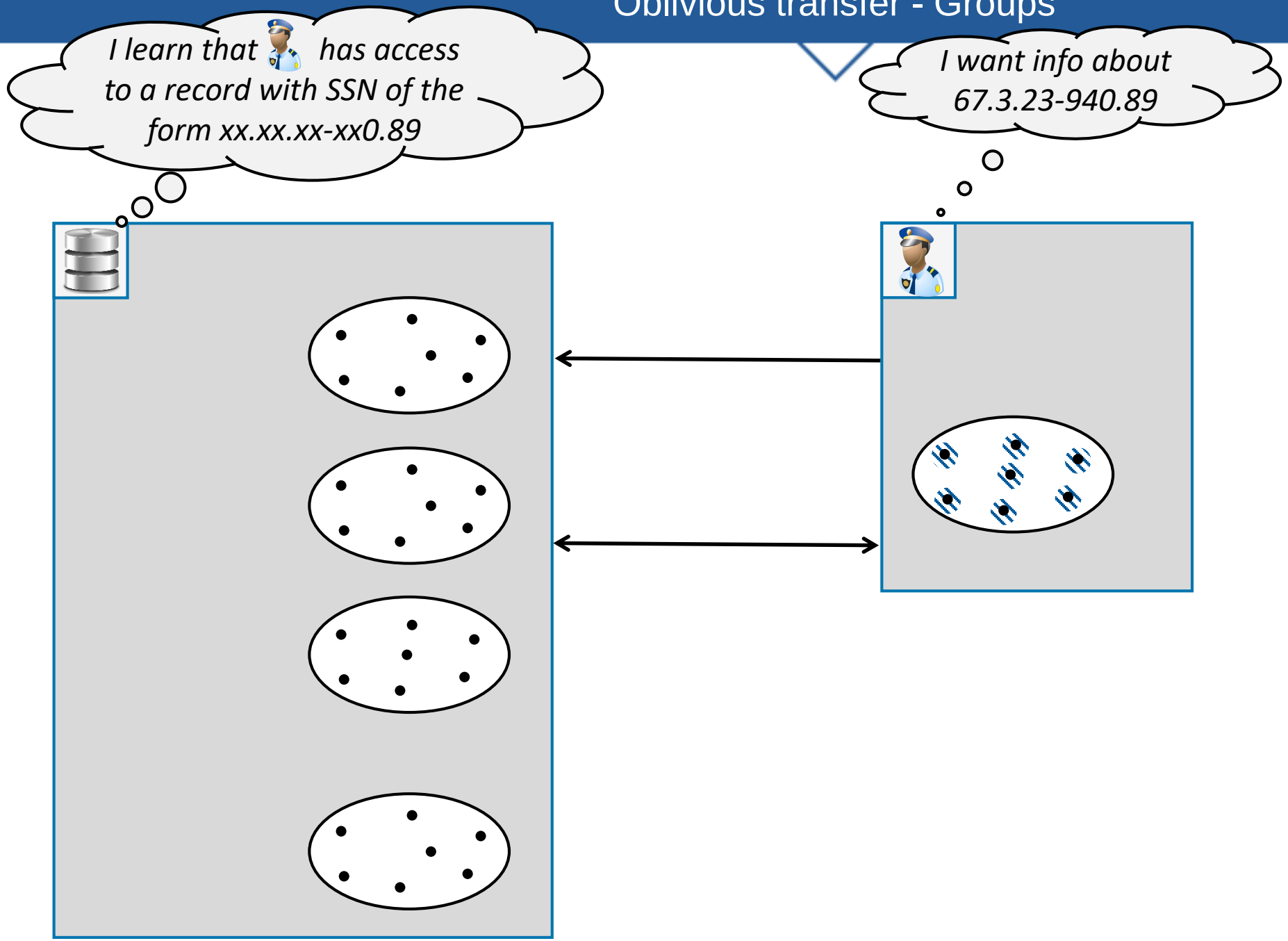
Oblivious transfer - Tension



Oblivious transfer - Concept

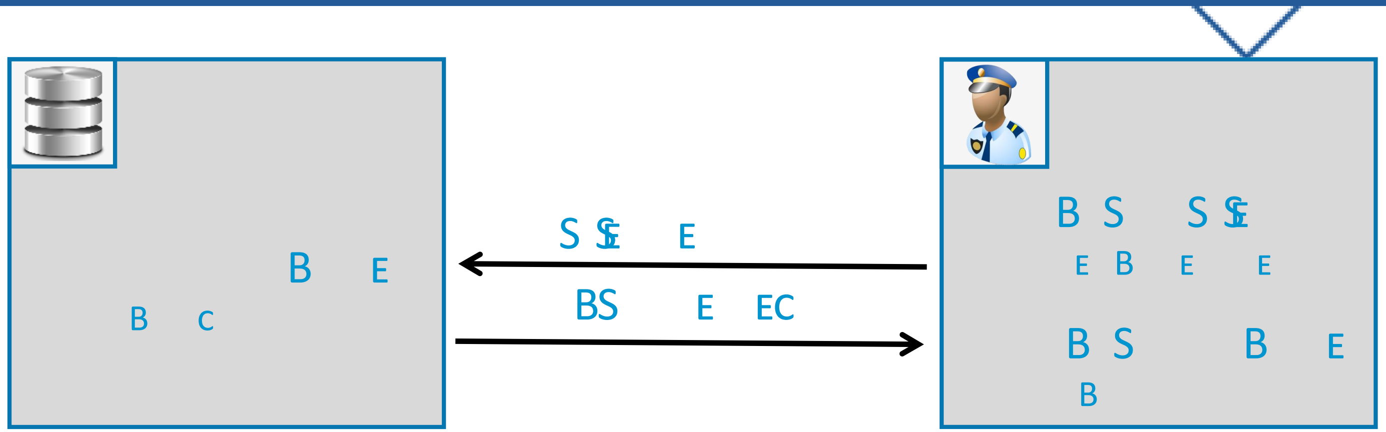


Oblivious transfer - Groups



- S S C B C E S
- S ES E S E BS E EC C

Oblivious transfer – Implementation & performance



E ES

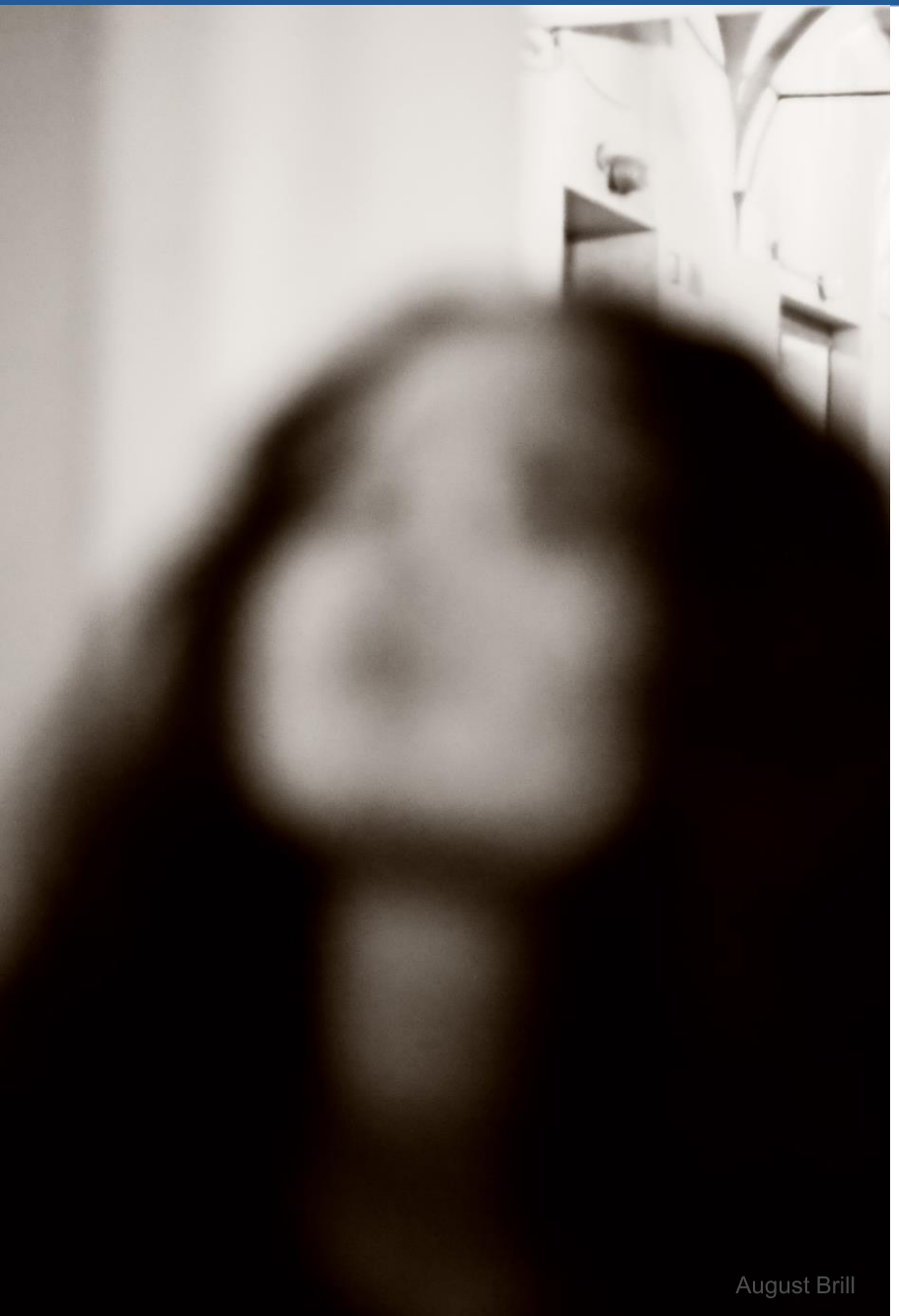
E C

	B S S S E O(log n)	B E O(log n*s)	B S B E O(s + log n)	B S S S E O(log n)	B E O(log n*s)	B S B E O(s + log n)	B S S S E O(log n)	B E O(log n*s)	B S B E O(s + log n)
B	C	C	C	C	C	C	C	C	C
B	C	C	C	C	C	C	C	C	C

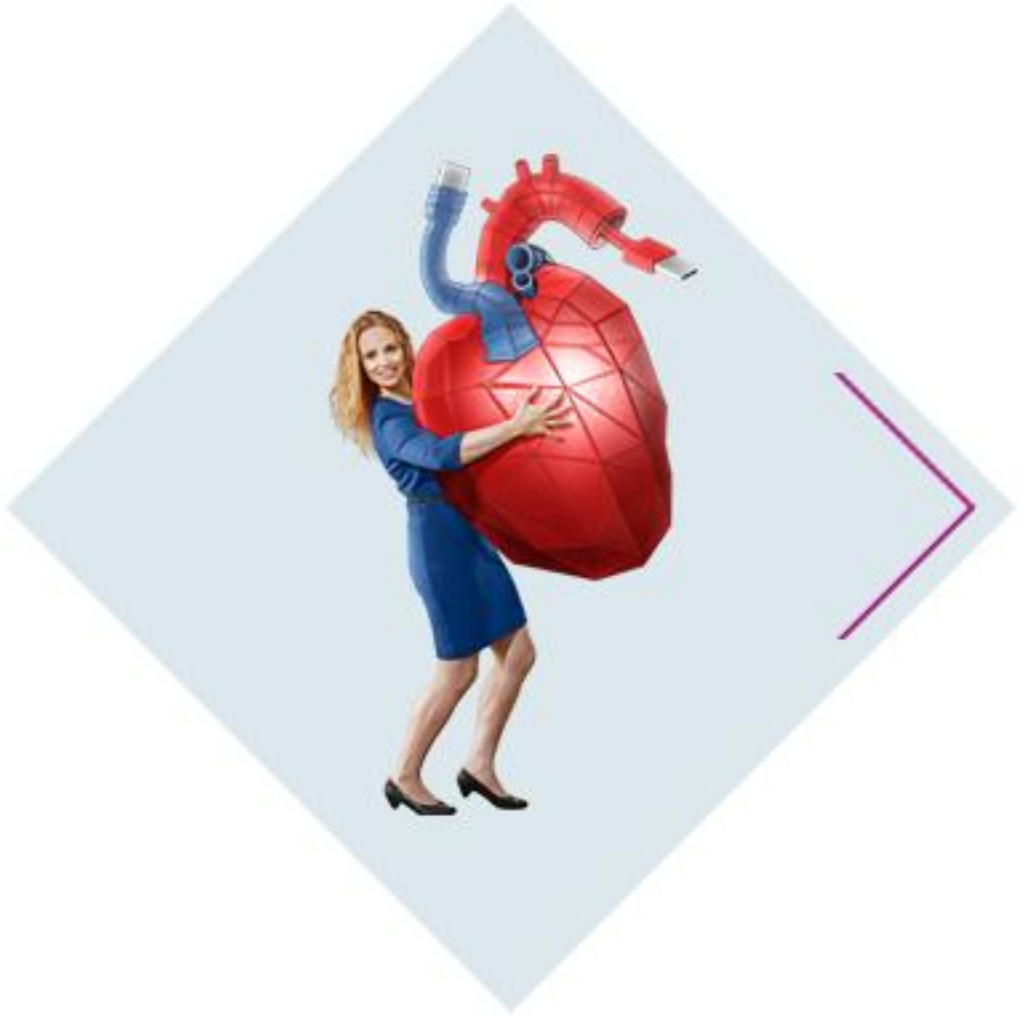
E S S S C E S B ES S B E B B ES C E CE B SB ES C S C E

S E S *Fast and Universally-Composable Oblivious Transfer and Commitment Scheme with Adaptive Security* E S E B S S E S E E E C *A Framework for Efficient and Composable Oblivious Transfer.* B C S E

Oblivious transfer



August Brill



Oblivious join

B E C C B

Joining personal data

- C CC CC B BES S
- S C

- BSSB SB E
- E ESC B CS E

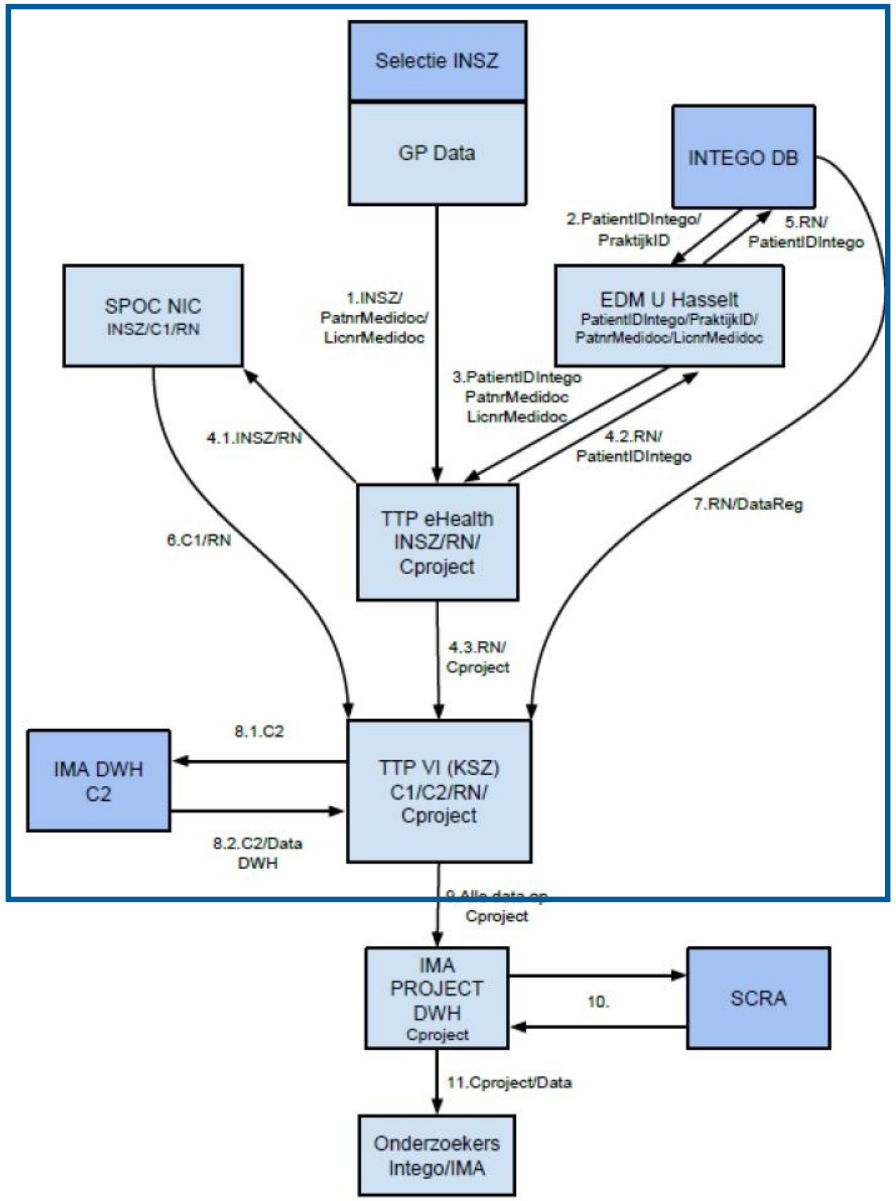
S S C S S
C E ES C B C
C B C C

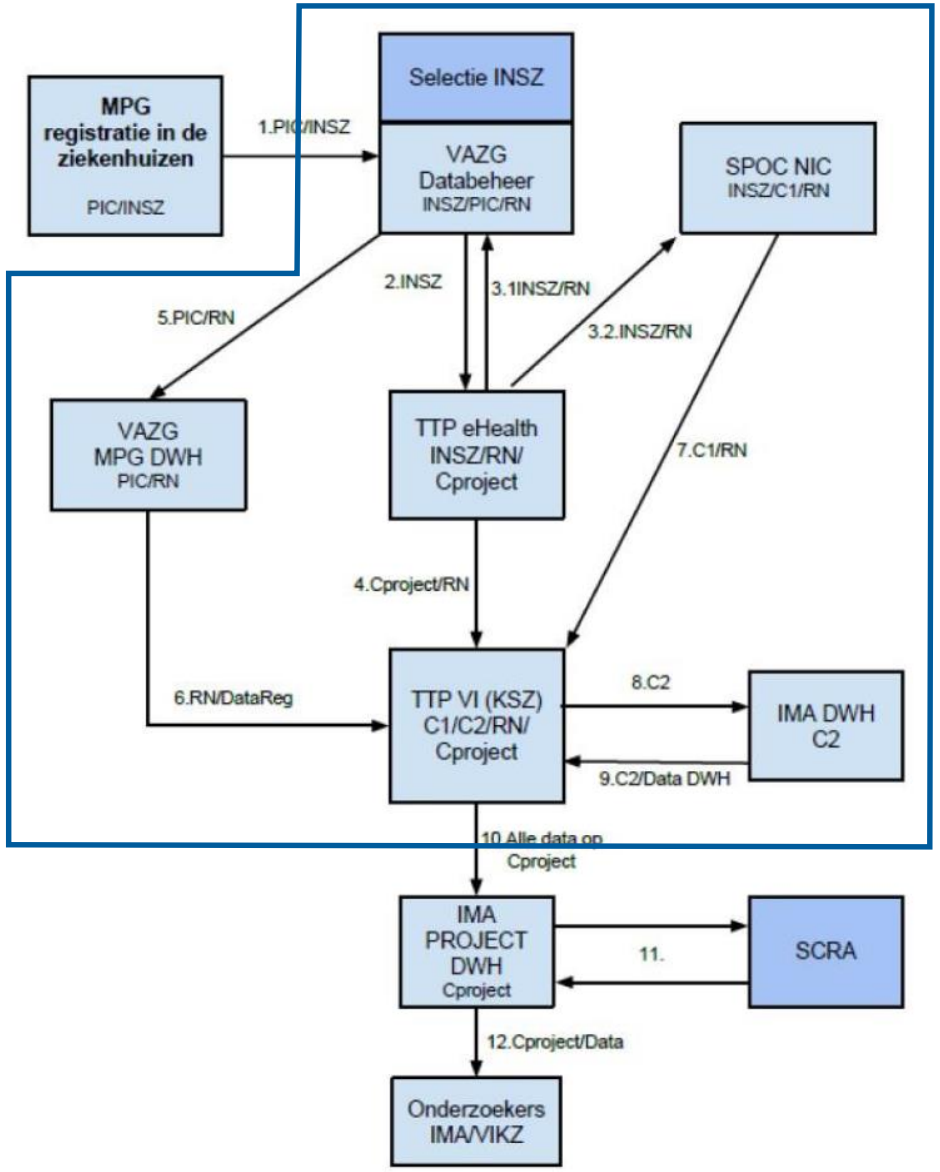
RSZ - ONSS - LSS

RSVZ

Belgian Cancer Registry

Joining personal data – Current practice





KSZ BCSS

S ES

E

S ES

S E

- 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

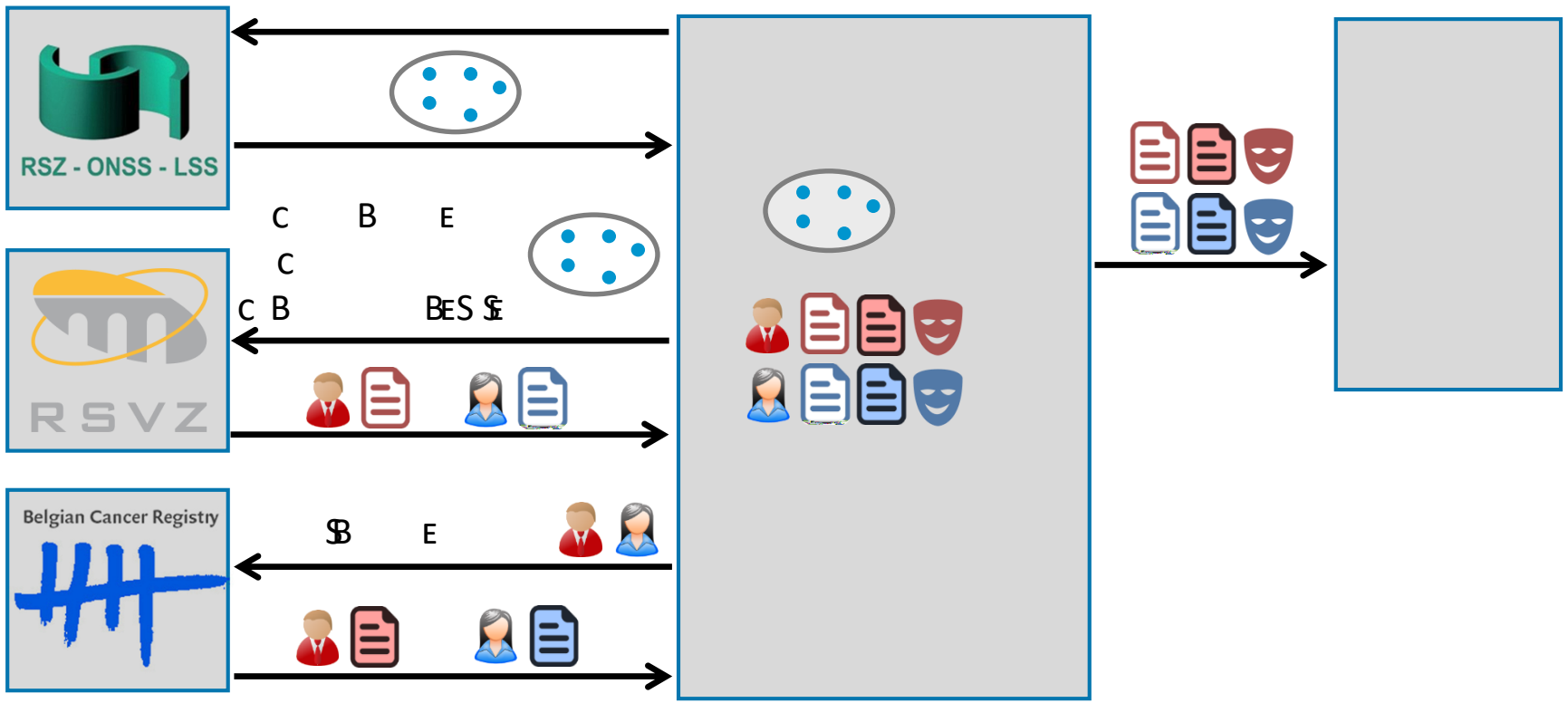
Required data

- Specific medical data
- Data about insurance as independent

Issues

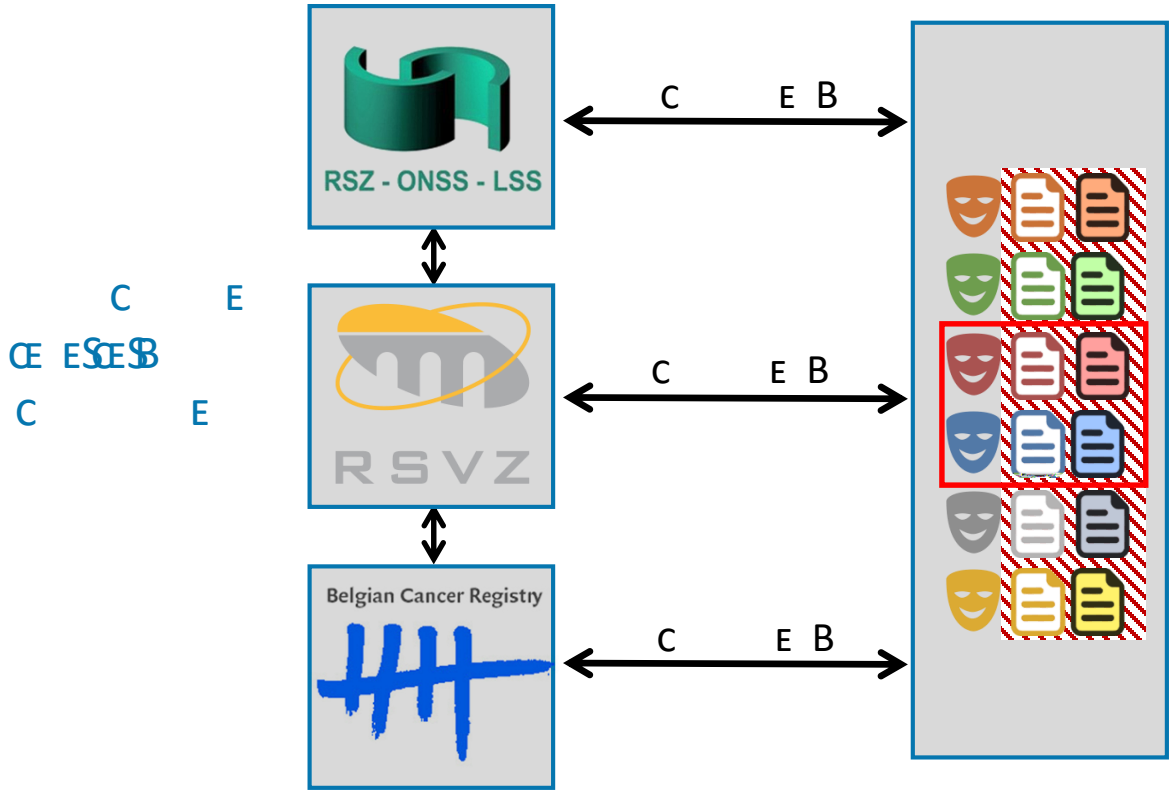
- Data leakage towards senders and/or TTP
- Extra intermediaries increase complexity

Potential traditional approach

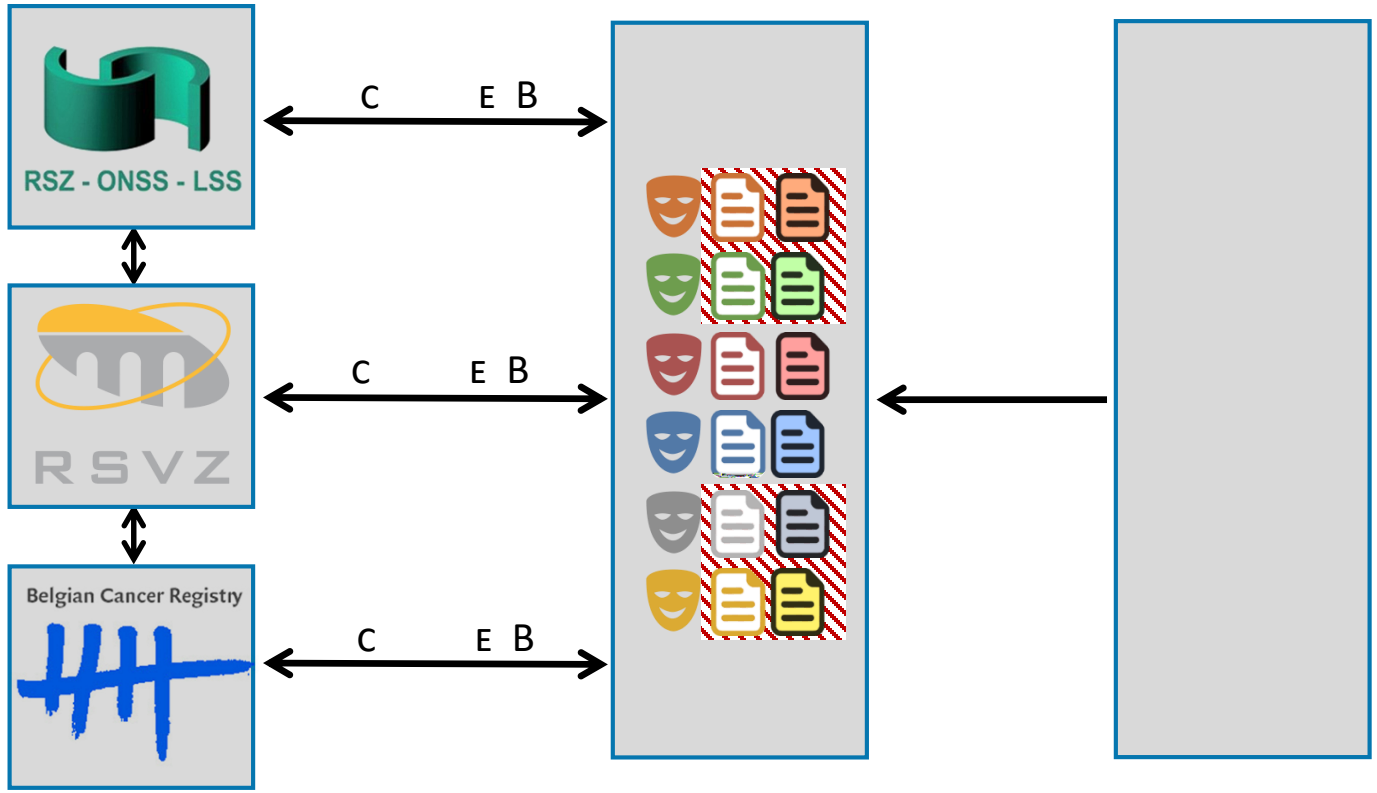


Smals
ICT for society

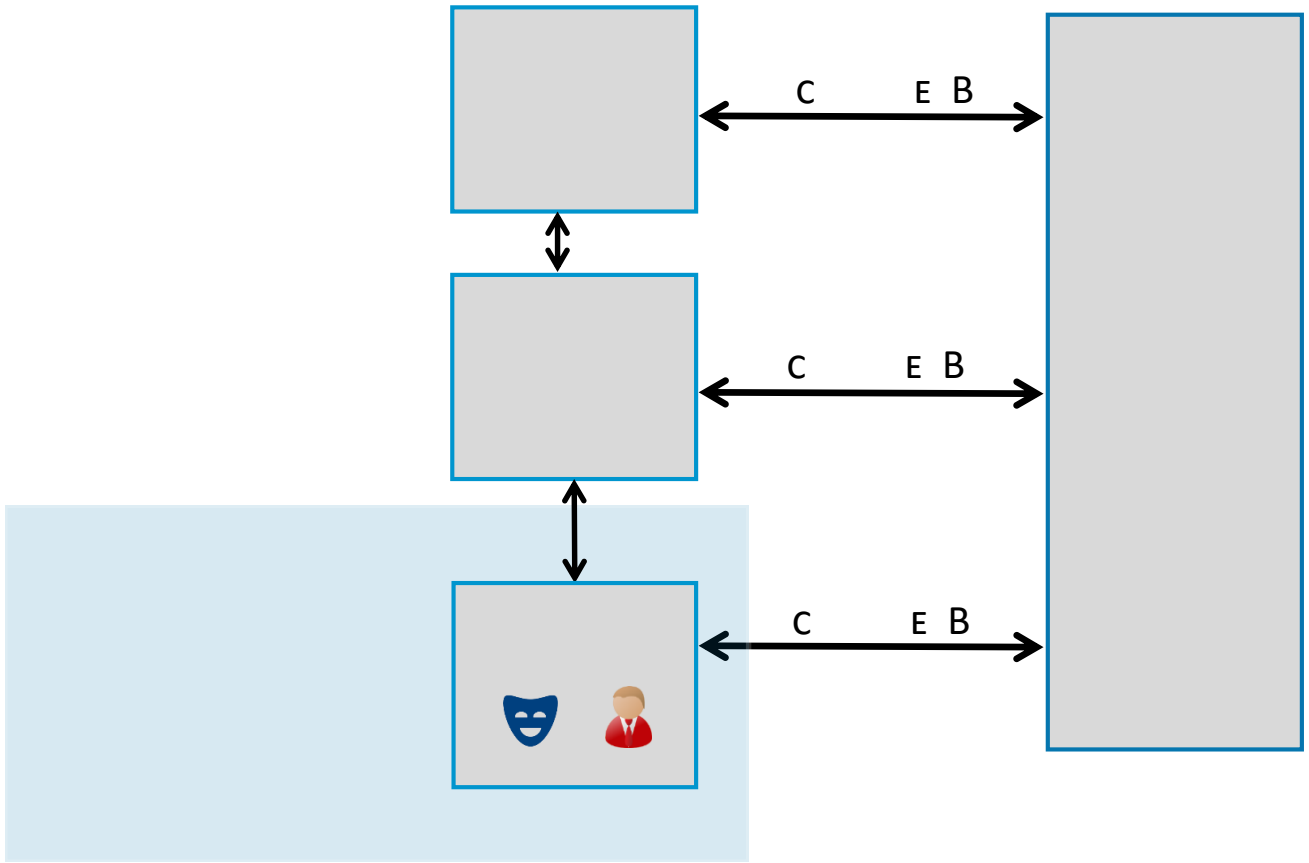
Oblivious join



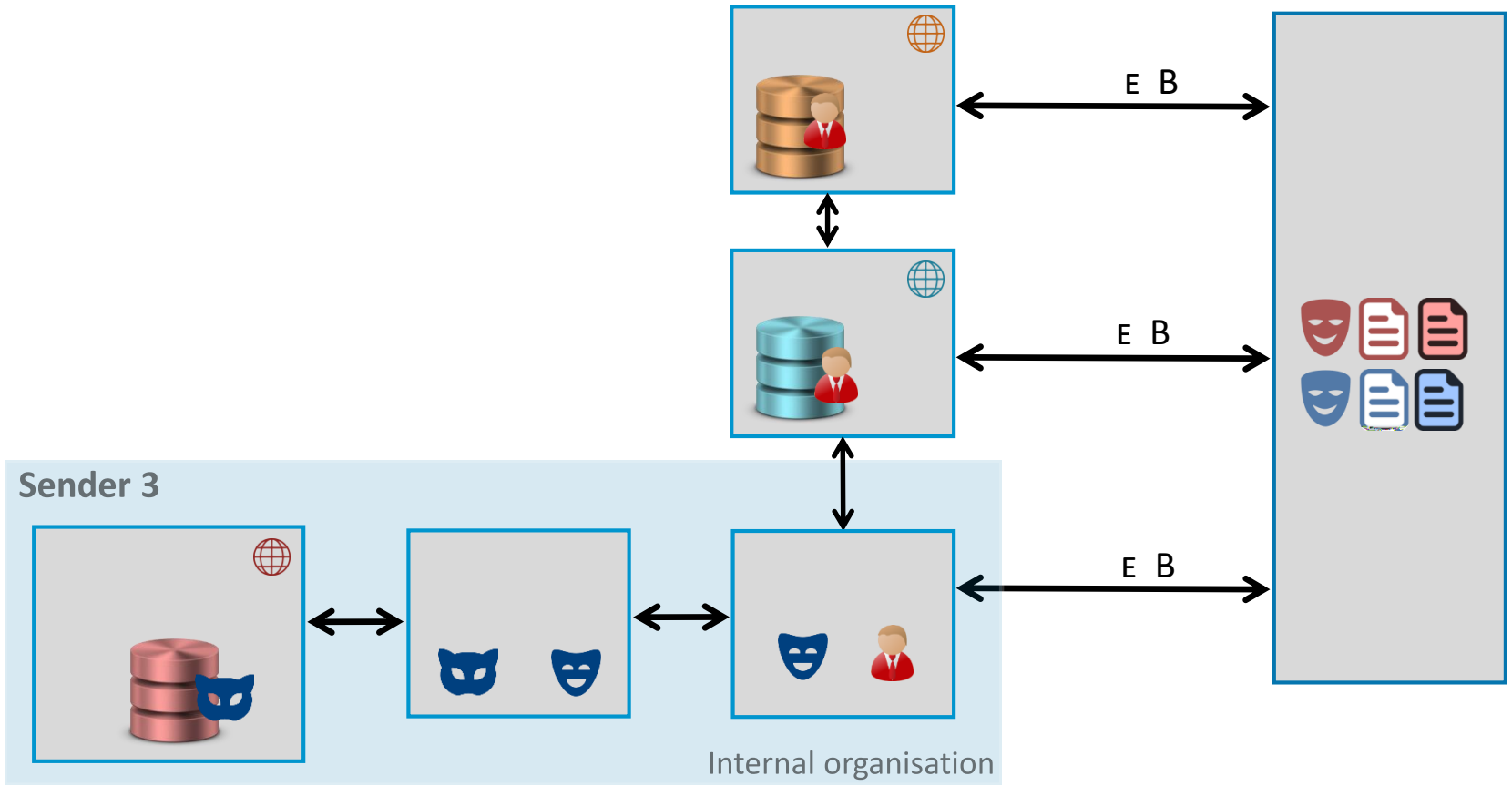
Oblivious join



Oblivious join

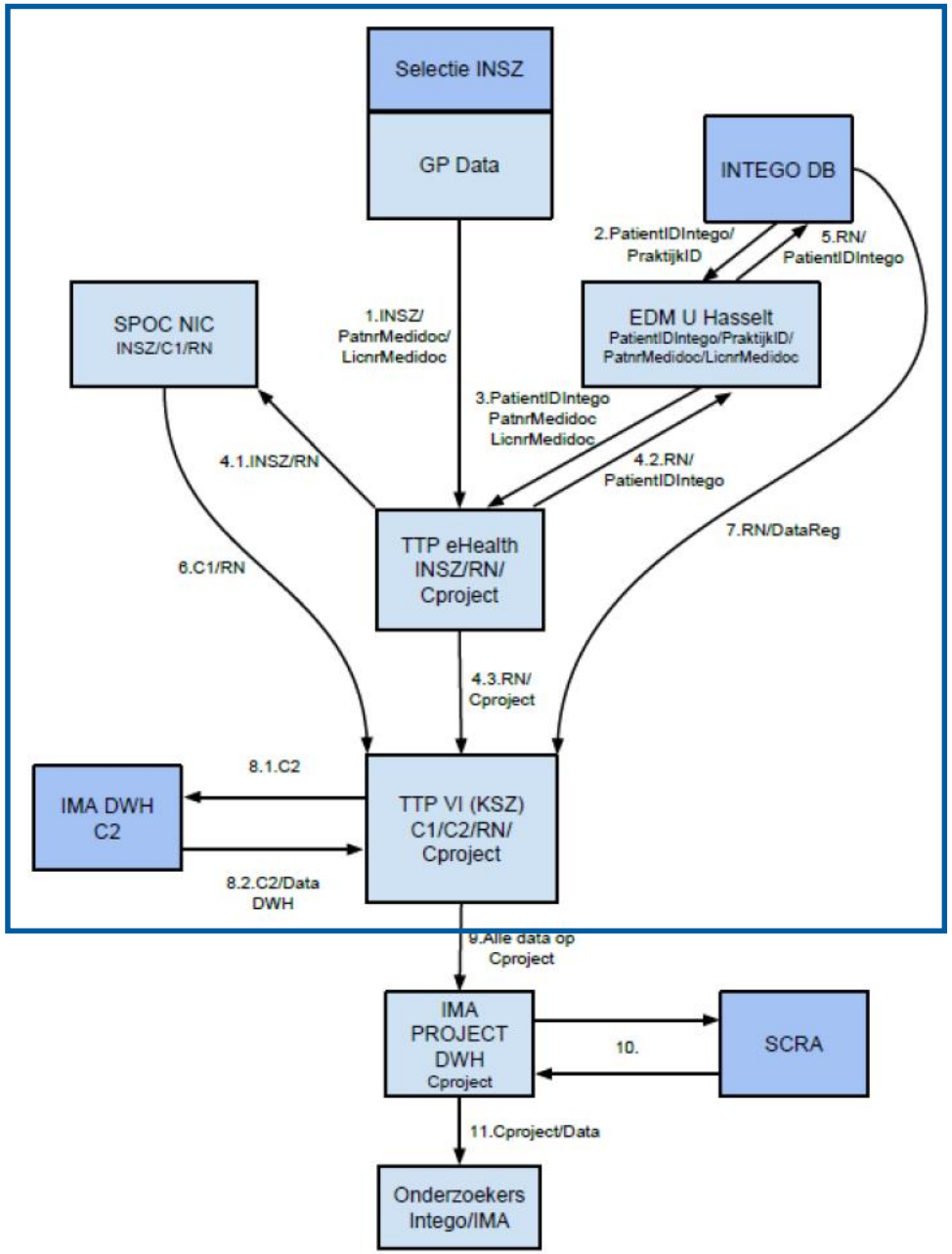


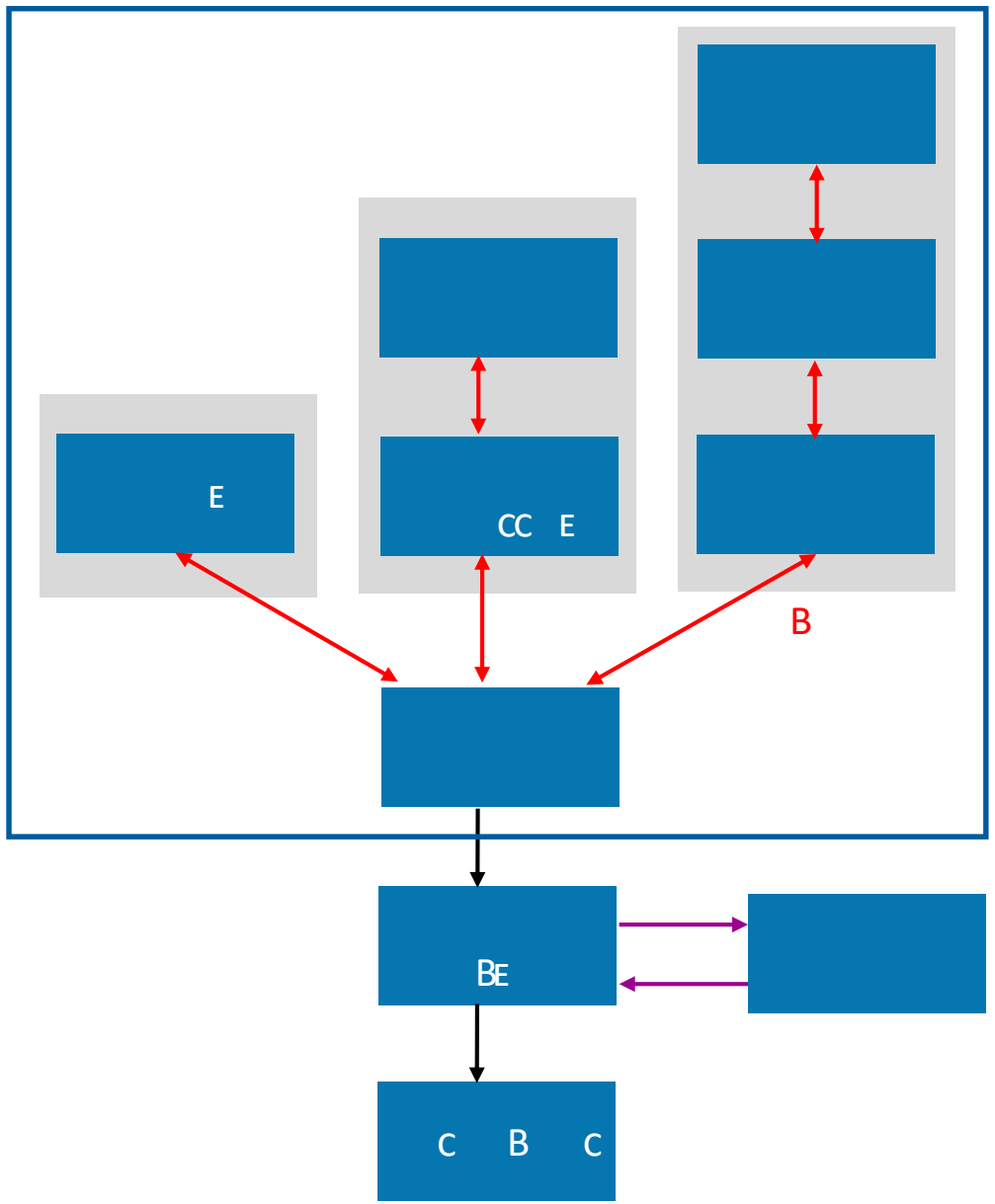
Oblivious join



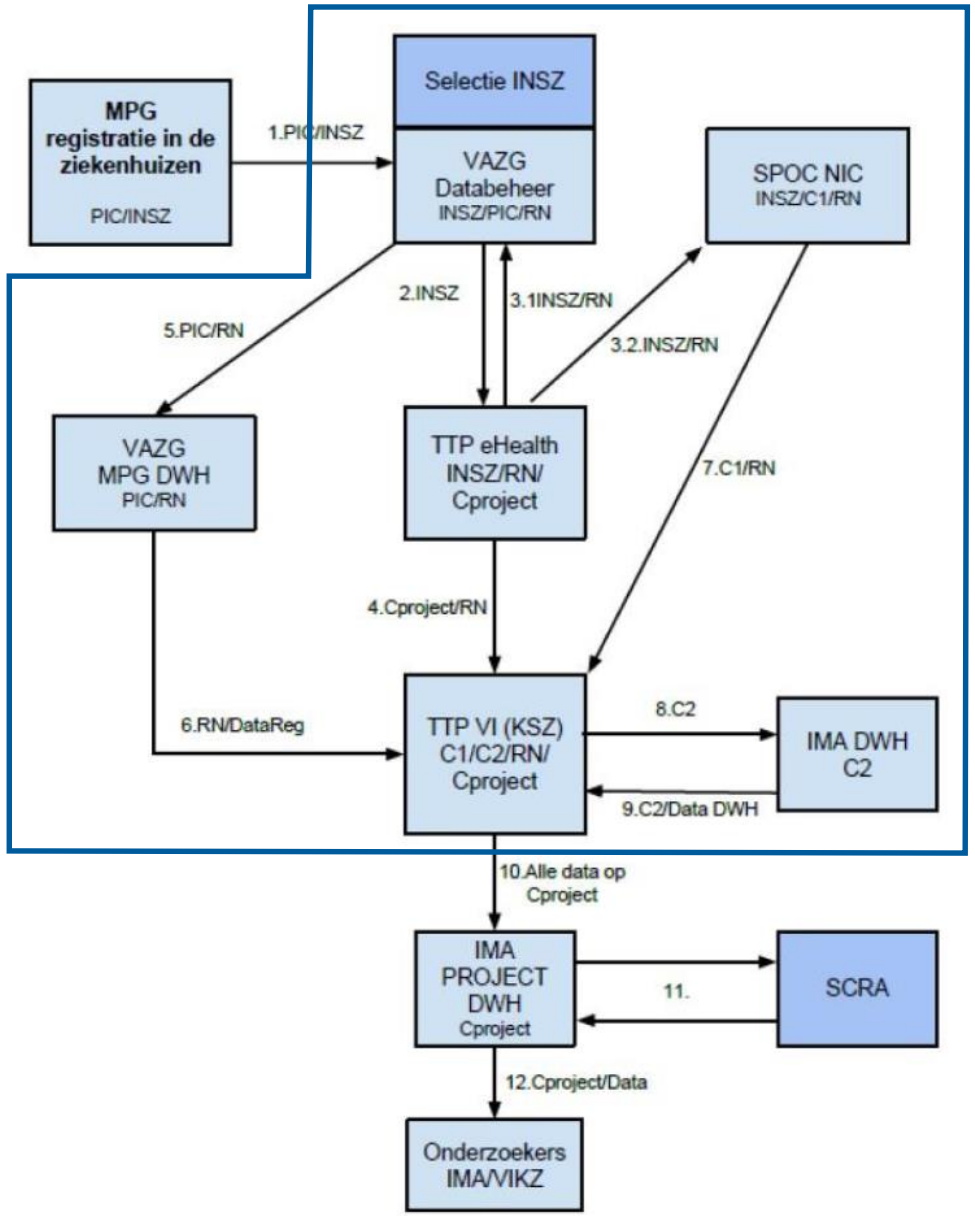
Smals
ICT for society

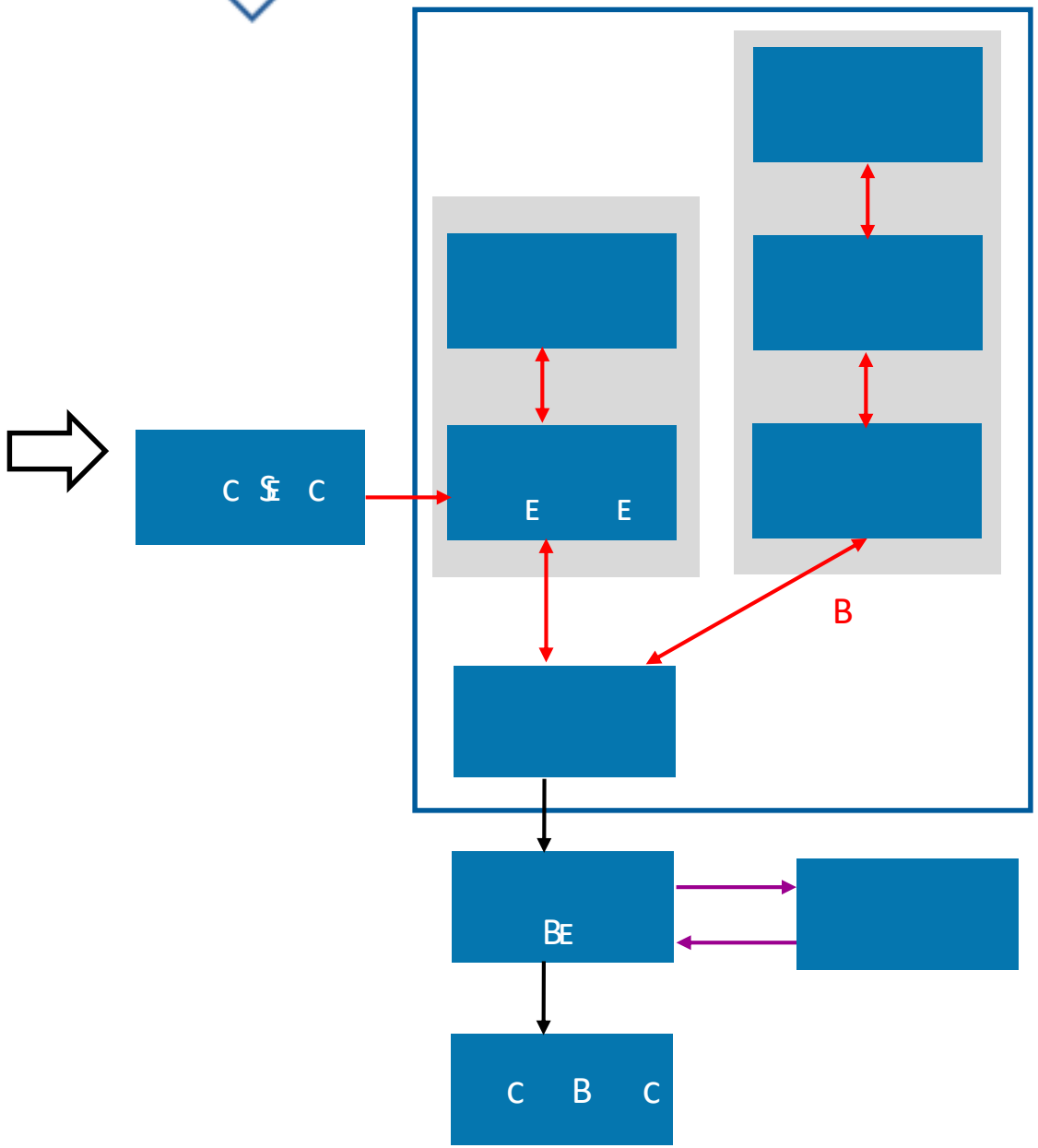
Current practice Vs. Oblivious join





Current practice Vs. Oblivious join

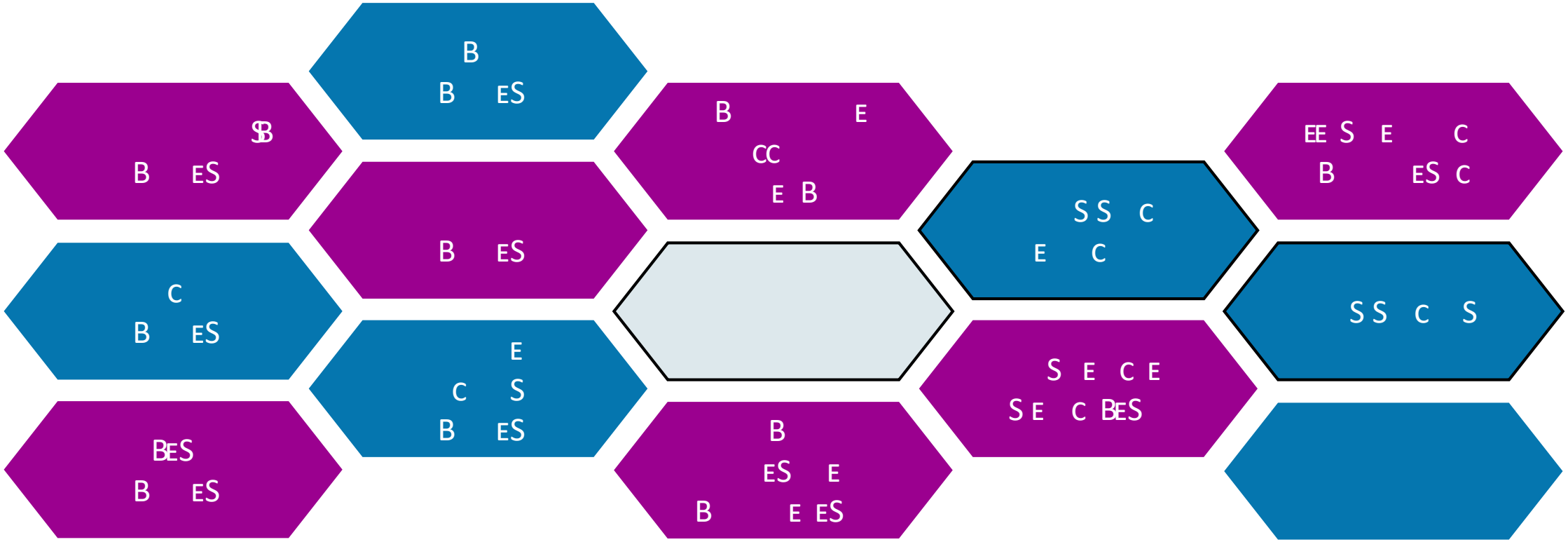




Oblivious join

-
-
-
-

Advanced cryptography



Advanced cryptography - Conclusions

kristof.verslype@smals.be

+32(0)2 7875376

www.smals.be
www.smalsresearch.be
www.cryptov.net (personal)