Privacy-enhancing technologies voor de publieke sector

21 december 2021

Kristof Verslype
Cryptograaf, PhD.
Smals Research

Smals
ICT for society

vrt NWS

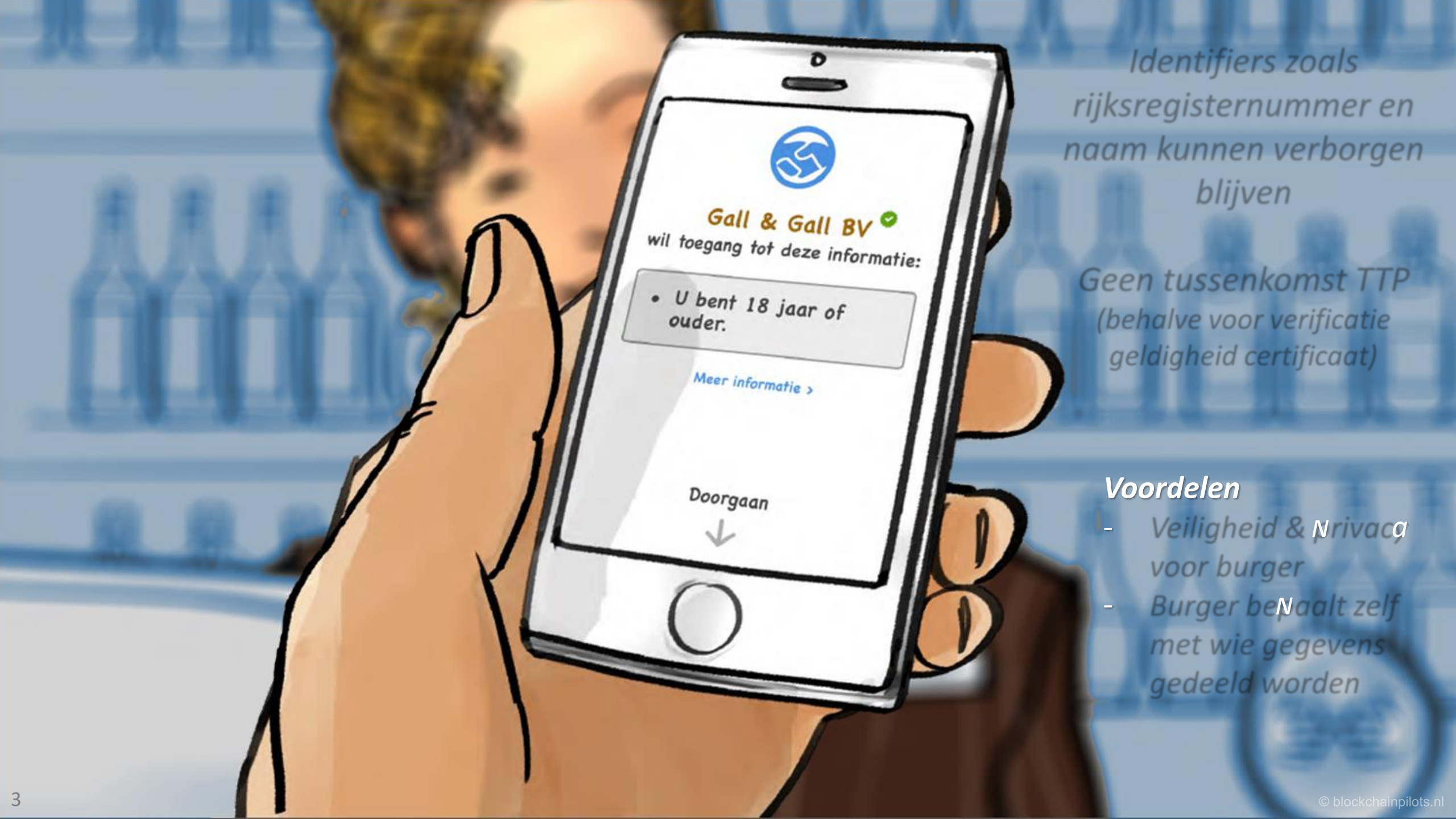
18 okt. 2021

Digitale portefeuille voor elke Belg tegen 2023

Staatssecretaris voor Digitalisering Mathieu Michel (MR) wil elke Belg tegen 2023 een "digitale portefeuille" geven. Dat zegt hij in een interview met Het Belang van Limburg. In die digitale portefeuille zouden alle officiële documenten gebundeld worden, zoals uw identiteitskaart en uw rijbewijs, maar bijvoorbeeld ook uw trouwboekje of een visum.

De bedoeling van de digitale portefeuille is om alle data van de verschillende overheden in ons land te koppelen en efficiënter beschikbaar te maken. En dat is nodig, benadrukt staatssecretaris Michel: "De digitale portefeuille is nodig omdat we in een complexe staat leven. De Belg moet niet het slachtoffer zijn van de complexiteit van onze overheid. Daarom hebben we tools nodig om het leven van de Belgen te vereenvoudigen."

https://www.vrt.be/vrtnws/nl/2021/10/18/digitale-portefeuille/



Identifiers zoals rijksregisternummer en naam kunnen verborgen blijven

Geen tussenkomst TTP (behalve voor verificatie geldigheid certificaat)

Voordelen

- *Veiligheid & Privacy voor burger*
- *Burger beslaalt zelf met wie gegevens gedeeld worden*

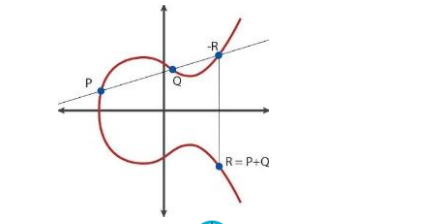
Privacy enhancing technologies

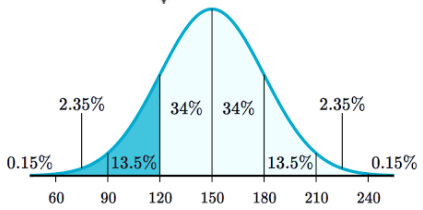
S

N *N* *a*

Doorgaans steunend op

- **Cryptografie**
  Beschermen van de gegevens m.b.v. wiskundige principes
- **Statistiek**
  Omzetten van grotere hoeveelheden data in inzichten





Stroomversnelling

- Al tientallen jaren academische speeltjes
- Recent ook ruimere aandacht
  - Theorie → praktisch bruikbaar
  - GDPR / AVG
  - Blockchain

Waarom?

Privacy / GDPR

Bescherming voor	Traditionele crypto	Traditionele crypto + PETs
Data at rest	✓	✓
Data in transit	✓	✓
Data in use	✗	?

- ► Privacyvereisten verzoenen met functionele vereisten
- ► Vermijden onbedoelde prijsgave persoonsgegevens
- ► Vereist *N* *a* *a*

Vertrouwen

N

N *N*

Dankzij PETs
- Minder TTPs (Trusted Third Parties)
- Minder vertrouwen in deze TTPs
- Samenwerkende partijen hoeven elkaar minder te vertrouwen

►► ***Partnership*** enhancing technologies

Efficiëntie

Elegantere processen
- Minder TTPs (Trusted Third Parties)
- Minder informatiestromen
- Maatwerk → uniforme aanpak

Vragen

Vraag 1
Hoe vinden we onze weg in het brede scala aan PETs?

Vraag 2
Wat zijn de toepassings-mogelijkheden in de publieke sector?

Vraag 3
Wat zijn de caveats?

Vraag voor u op einde webinar (multiple-choice)
Welke PETs hebben volgens u het meest potentieel en verdienen dus meer aandacht?

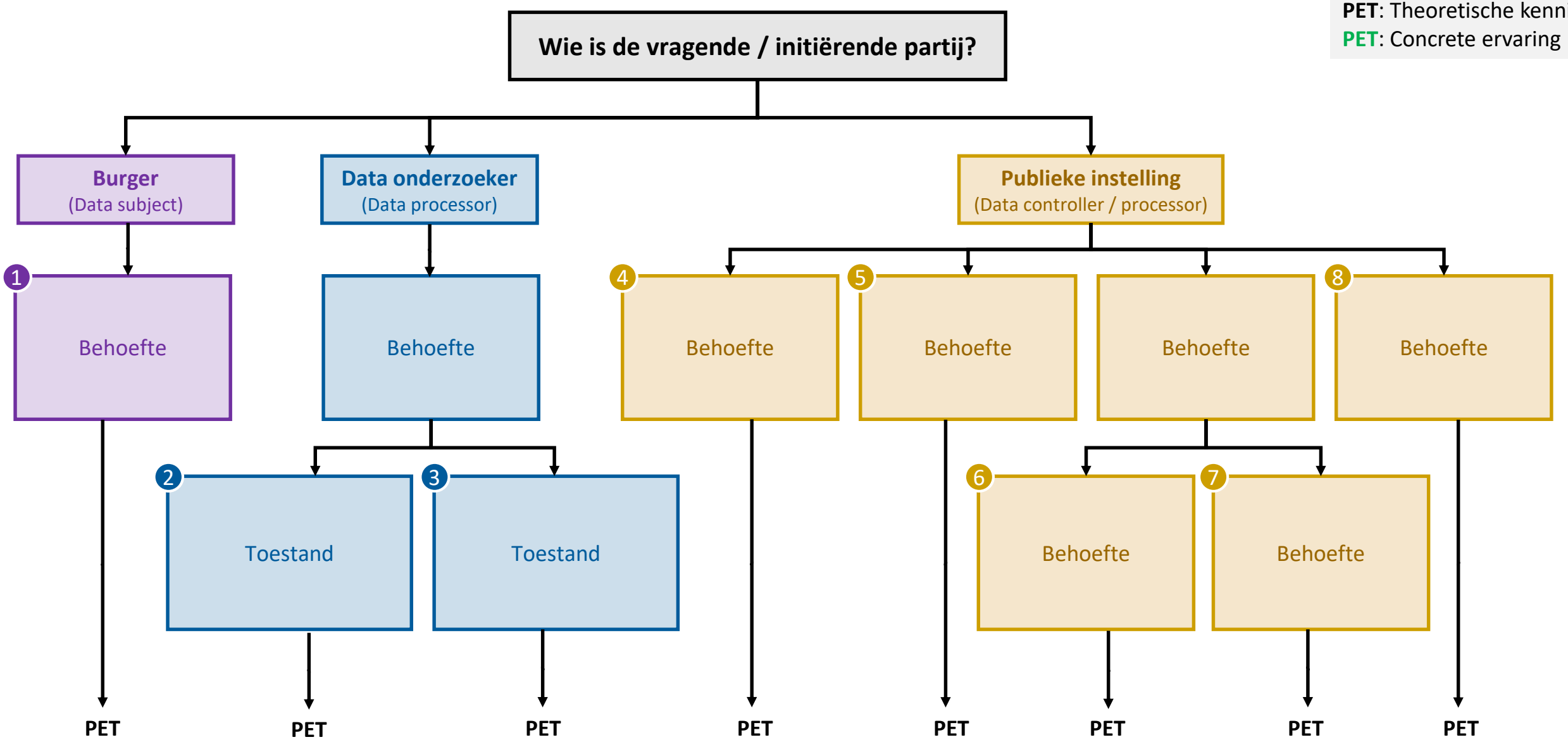
Specifieke vragen kunt u kwijt in de chat en komen op het einde aan bod.

Disclaimer
- Geen volledigheid, eerder ter inspiratie/leidraad
- Webinar gaat niet in op PETs voor machine learning
- Webinar is niet diep technisch

Smals ICT for society

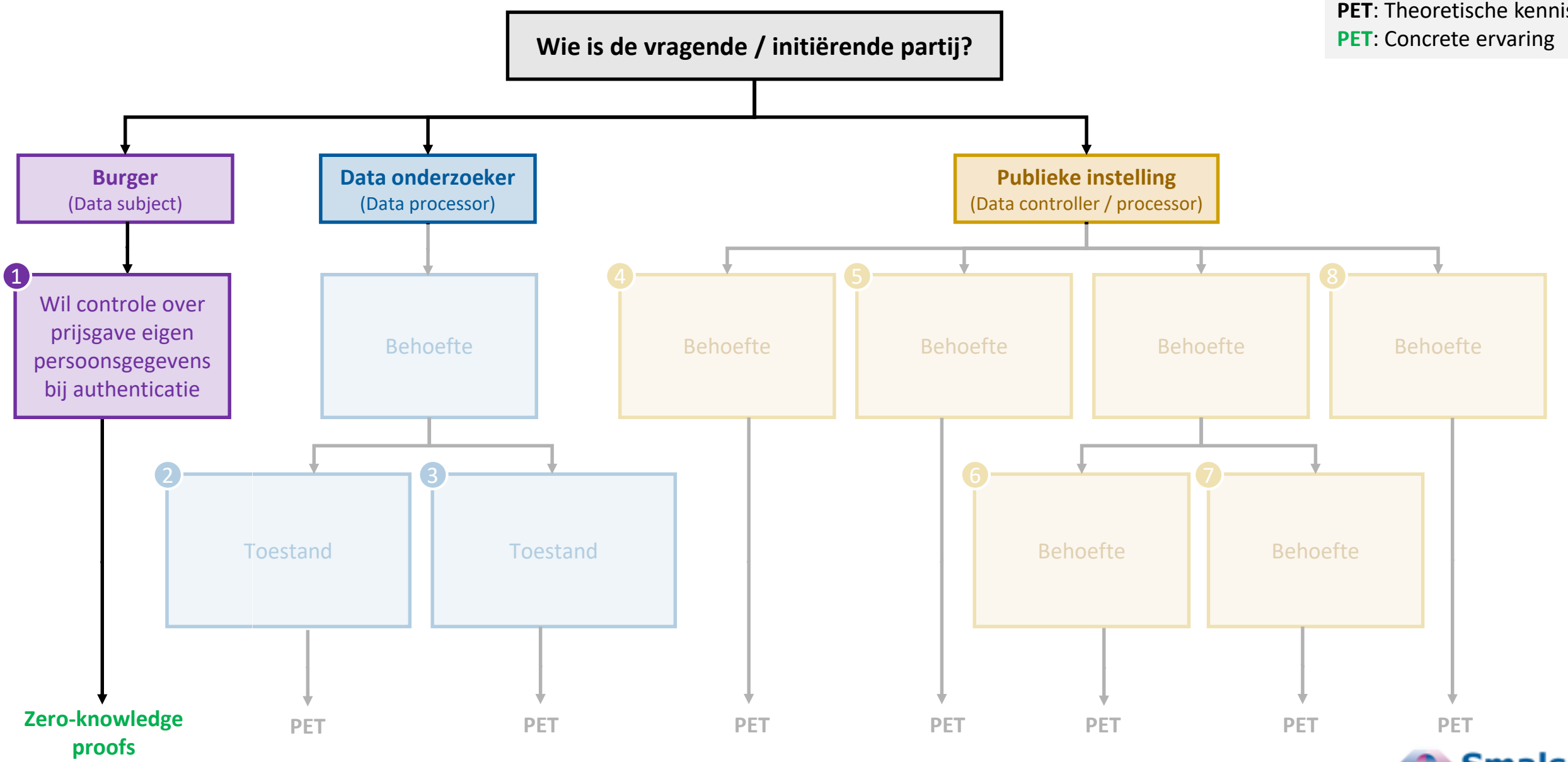
Selectieboom

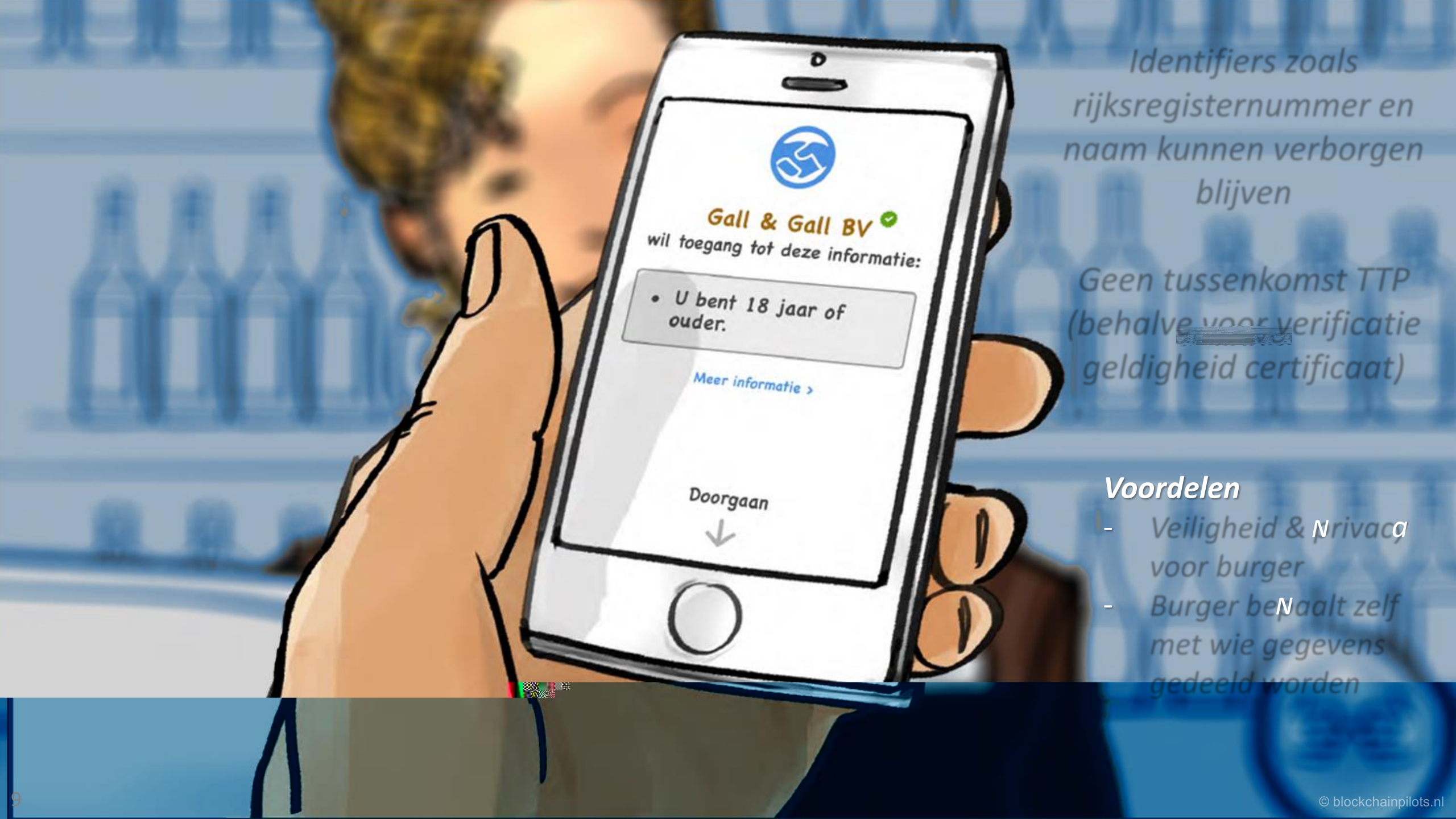
PET: Theoretische kennis
PET: Concrete ervaring



Selectieboom

PET: Theoretische kennis
PET: Concrete ervaring





Identifiers zoals rijksregisternummer en naam kunnen verborgen blijven

Geen tussenkomst TTP (behalve voor verificatie geldigheid certificaat)

Voordelen

- *Veiligheid & Privacy voor burger*
- *Burger beslaalt zelf met wie gegevens gedeeld worden*

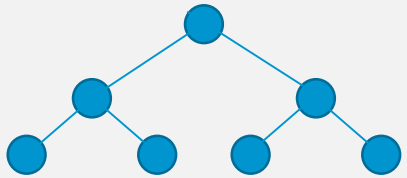
Selectieve prijsgave van persoonsgegevens

- vb. “*Ik woon in Vlaams-Brabant, ben 18+ en heb een rijbewijs*”
- Zonder prijsgave van anders persoonsgegevens
- Zonder medeweten TTP

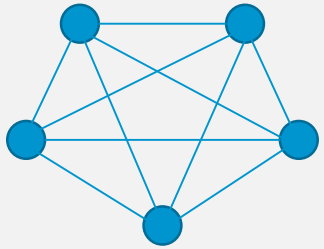
Fundament voor

Self-Sovereign Identity (SSI)

- Burger krijgt controle over haar digitale identiteiten (diploma’s, identiteitskaart, …)
- SSI is een filosofie, geen technologie
- Geen exclusiviteit van blockchain



PKI infrastructuur



Blockchain

Andere toepassingen

- Electronic voting, anonymous money
- Blockchain technologieën & toepassingen (vb. virtuele munten)

Alexandr Ivanov

Zero-knowledge proofs

Worden reeds gebruikt

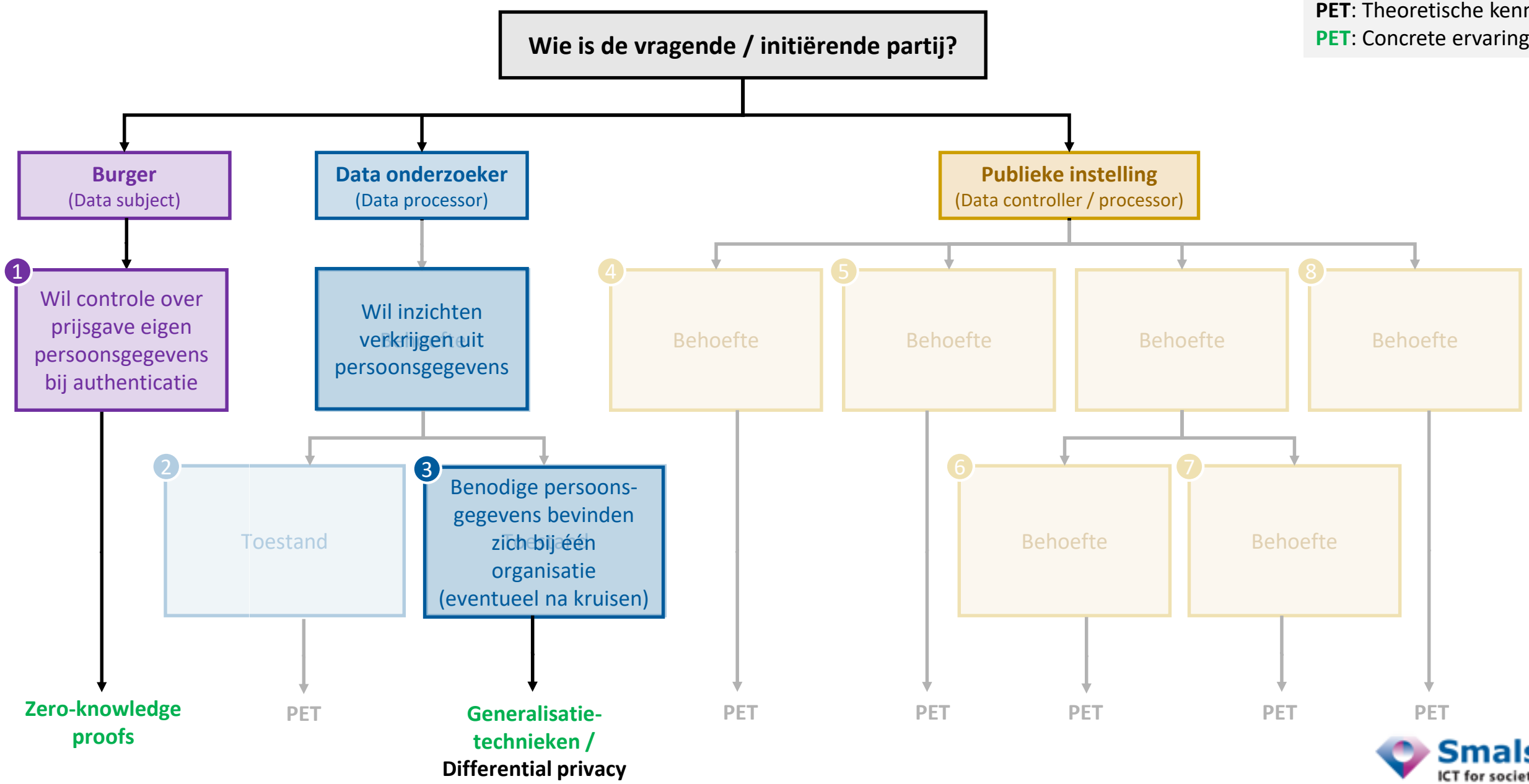
Hebben potentieel binnen de ambities van de huidige regering

Opletten voor “ *a* ”

Smals ICT for society

Selectieboom

PET: Theoretische kennis
PET: Concrete ervaring



Onderzoeker wil inzichten bekomen uit reeds gecentraliseerde persoonsgegevens

Onderzoeker

- Wil inzichten bekomen uit gezondheidsdata, socio-economische data, etc. van burgers
- Krijgt enkel toegang tot minimaal noodzakelijke, gedeïdentificeerde gegevens
- Data set mogelijk nog steeds erg gevoelig

De data gaan naar de berekeningen

Generalisatietechnieken (1998)
(aka “anonimisatietechnieken”)

Vervagen van gegevens in de data set

Smals
ICT for society

Generalisatietechnieken

SSN	Race	BirthDate	Gender	ZIP	Problem
021-57-1445	black	9/20/1965	male	02141	short of breath
021-77-8034	black	2/14/1965	male	02141	chest pain
107-21-0876	black	10/23/1965	female	02138	painful eye
021-37-1573	black	8/24/1965	female	02138	wheezing
021-54-4229	black	11/7/1964	female	02138	obesity
117-26-3042	black	12/1/1964	female	02138	chest pain
127-91-4819	white	10/23/1964	male	02138	short of breath
270-89-1234	white	3/15/1965	female	02139	hypertension
021-45-7854	white	8/13/1964	male	02139	obesity
021-08-2839	white	5/5/1964	male	02139	fever
117-61-0504	white	2/13/1967	male	02138	vomiting
021-668-9440	white	3/21/1967	male	02138	back pain

Race	BirthDate	Gender	ZIP	Problem
black	1965	male	02141	short of breath
black	1965	male	02141	chest pain
person	1965	female	0213*	painful eye
person	1965	female	0213*	wheezing
black	1964	female	02138	obesity
black	1964	female	02138	chest pain
white	1964	male	0213*	short of breath
person	1965	female	0213*	hypertension
white	1964	male	0213*	obesity
white	1964	male	0213*	fever
white	1967	male	0213*	vomiting
white	1967	male	0213*	back pain

Voorbeelden technologieën:
k-anonymity, l-diversity en t-closeness

Meer generalisatie
→ hogere privacy, lager nut

Nuttig om identificatierisco te reduceren,
Verwacht geen nuttige geanonimiseerde data

arx.deidentifier.org

Onderzoeker wil inzichten bekomen uit reeds gecentraliseerde persoonsgegevens

Onderzoeker

- Wil inzichten bekomen uit gezondheidsdata, socio-economische data, etc. van burgers
- Krijgt enkel toegang tot minimaal noodzakelijke, gedeïdentificeerde gegevens
- Data set mogelijk nog steeds erg gevoelig

De data gaan naar de berekeningen

Generalisatietechnieken (1998)
(aka “anonimisatietechnieken”)

Vervagen van gegevens in de data set

De berekeningen gaan naar de data

Differential privacy (2006)
Wiskundig onderbouwd

Vervagen gegevens in resultaat query

Smals ICT for society

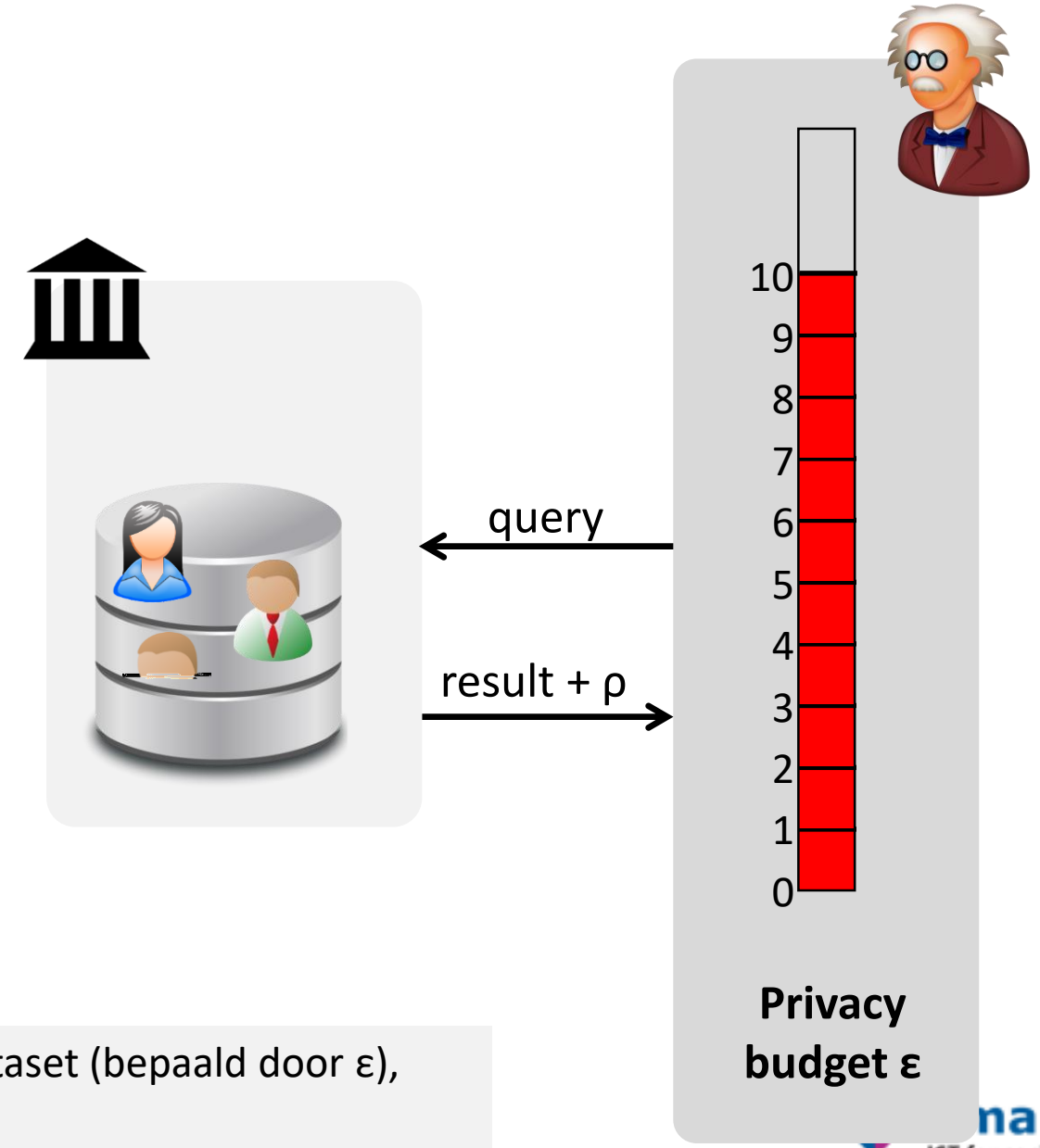
Differential privacy

Query 1
Veel ruis, dus minder exact
$\varepsilon = \varepsilon - 1$

Query 2
Weinig ruis, dus vrij exact
$\varepsilon = \varepsilon - 6$

Query 3
Ruis tussenin, exactheid ook
$\varepsilon = \varepsilon - 3$

Geen verdere queries toegelaten

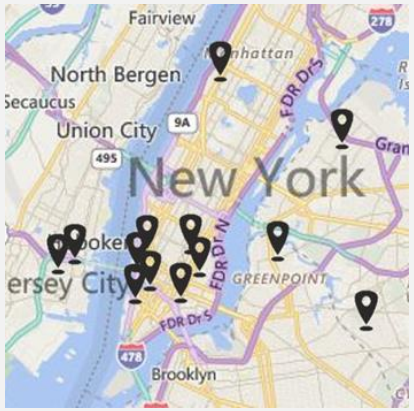


Niveau van privacy gegarandeerd voor elke burger in dataset (bepaald door ε), zelfs indien onderzoeker query resultaten samenlegt

Differential privacy – Real-world toepassingen

Microsoft

PrivTree
Blurring your “where” for location privacy



Uber

Enforces differential privacy for real-world SQL queries (by its staff)

Eigenschappen
- Op legacy infra
- SQL queries herschreven
- Open source

LinkedIn

Audience Engagements API
“ *a*
a *a*
”

To enable marketing analytics

Google RAPPOR
Crowdsourcing statistics from end-user client software while preserving the privacy of individual users.

Eigenschappen
- Open source
- Chrome homepage study met 14M gebruikers

Smals ICT for society

Differential privacy – Correct gebruik

Privacy

- Apple: “ N a N a”
- Code waarde closed source (= black box = “ ”)
- Na 6 maand onderzoek: “ N a ”)
- a

Nauwkeurigheid

AP

People, homes vanish due to 2020 census’ new privacy method

By MIKE SCHNEIDER October 31, 2021

Click to copy

Harvard researchers: - Principes zoals ‘ niet gegarandeerd
- “ a N N a N N ”

Aandachtspunten

- Gebruik DP enkel waarvoor bedoeld: Uitvoeren van 1 of beperkt aantal statistische queries op een DB
- Keuze van ε cruciaal

Over slecht gebruik DP

Domingo-Ferrer, J., Sánchez, D. and Blanco-Justicia, A., 2021. N a

C

, (7), pp.33-35.

https://www.wired.com/story/apple-differential-privacy-shortcomings/
https://apnews.com/article/religion-wisconsin-new-york-tampa-florida-68c96e7eb701da74ae7c8df3c3476705
https://apnews.com/article/business-census-2020-technology-e701e313e841674be6396321343b7e49

Onderzoeker wil inzichten bekomen uit reeds gecentraliseerde persoonsgegevens

Onderzoeker

- Wil inzichten bekomen uit gezondheidsdata, socio-economische data, etc. van burgers
- Krijgt enkel toegang tot minimaal noodzakelijke, gedeïdentificeerde gegevens
- Data set mogelijk nog steeds erg gevoelig

De data gaan naar de berekeningen

Generalisatietechnieken (1998)
(aka “anonimisatietechnieken”)

Vervagen van gegevens in de data set

De berekeningen gaan naar de data

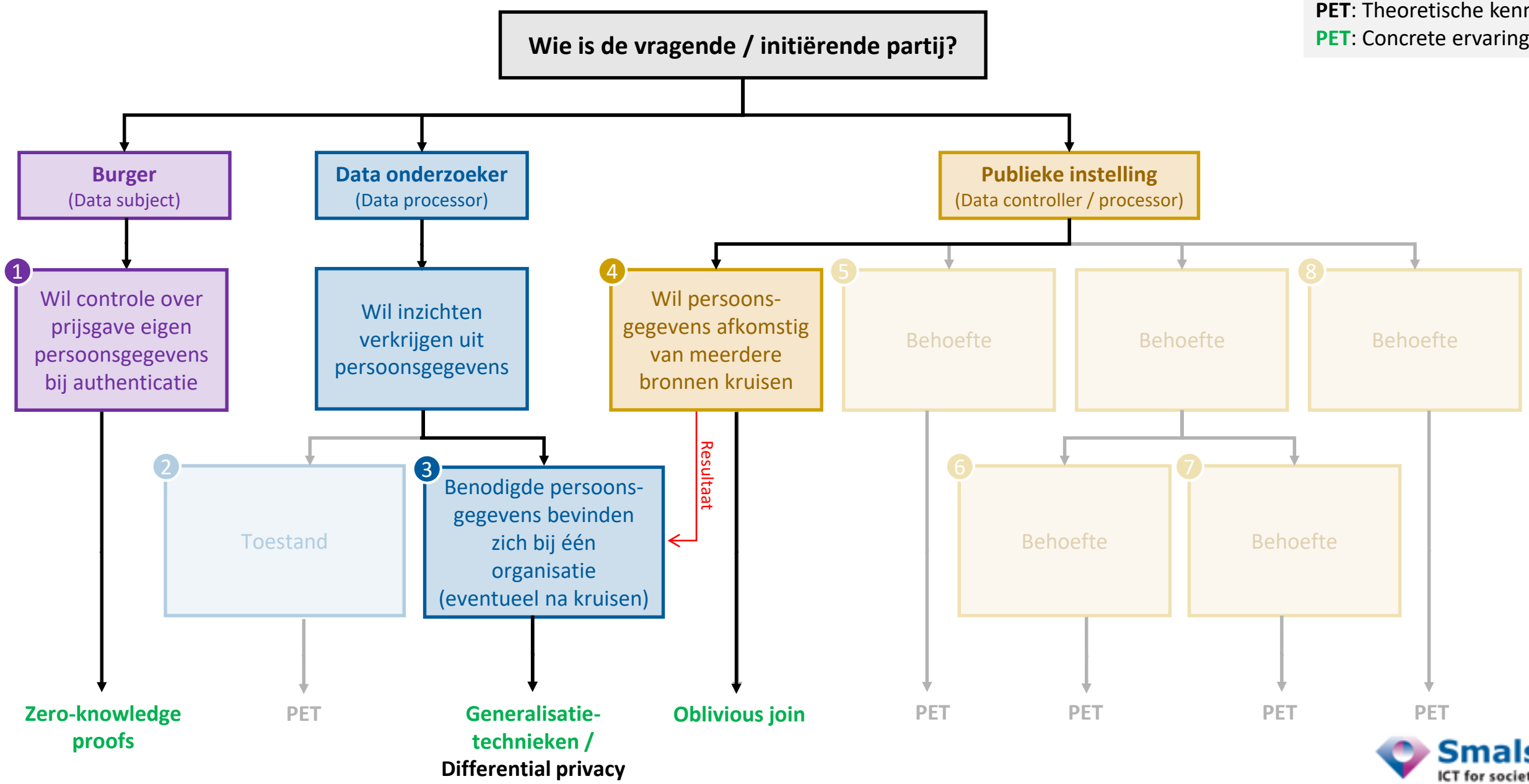
Differential privacy (2006)
Wiskundig onderbouwd

Vervagen gegevens in resultaat query

Kunnen waardevol zijn
Vandaag toepasbaar
Opletten voor correcte toepassing

Selectieboom

PET: Theoretische kennis
PET: Concrete ervaring



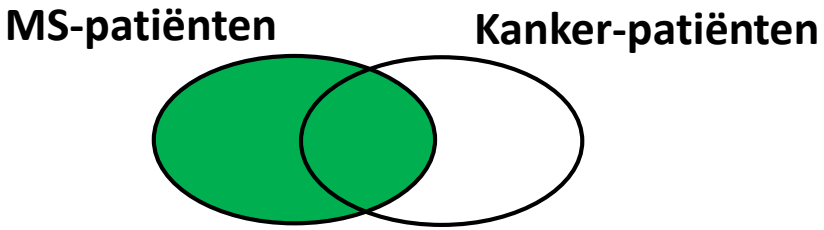
Reëel voorbeeld

Onderzoeksvraag

Hebben MS-patienten die medicijnen met molecule teriflunomide of alemtuzumab een verhoogd kankerrisico in vergelijking met MS-patiënten die met andere medicatie behandeld worden?

Betrokken burgers

- Alle MS-patiënten (± 15 000 patiënten)



Benodigde data

- Gegevens met betrekking tot medicatie (IMA)
- Gegevens met betrekking tot kanker (SKR)

Databronnen (zenders):

IMA-AIM

Belgian Cancer Registry

Hoe kan SKR enkel de relevante records (over burgers in doorsnede) aanleveren zonder te weten te komen wie MS-heeft?

Privacy-vriendelijk en efficiënt kruisen en deïdentificeren van persoonsgegevens in het kader van specifieke onderzoeksvragen

Observaties huidige werkwijze

- Privacy
  Goed nadenken om data lekken te vermijden
- Efficiëntie
  Complex, op maat

→ **Veilige, uniforme aanpak met OJ**

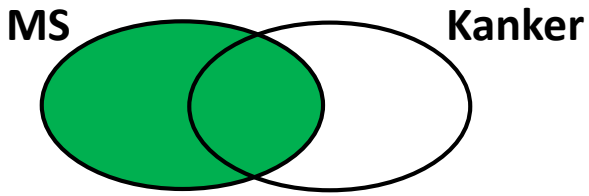
Oblivious join - Concept

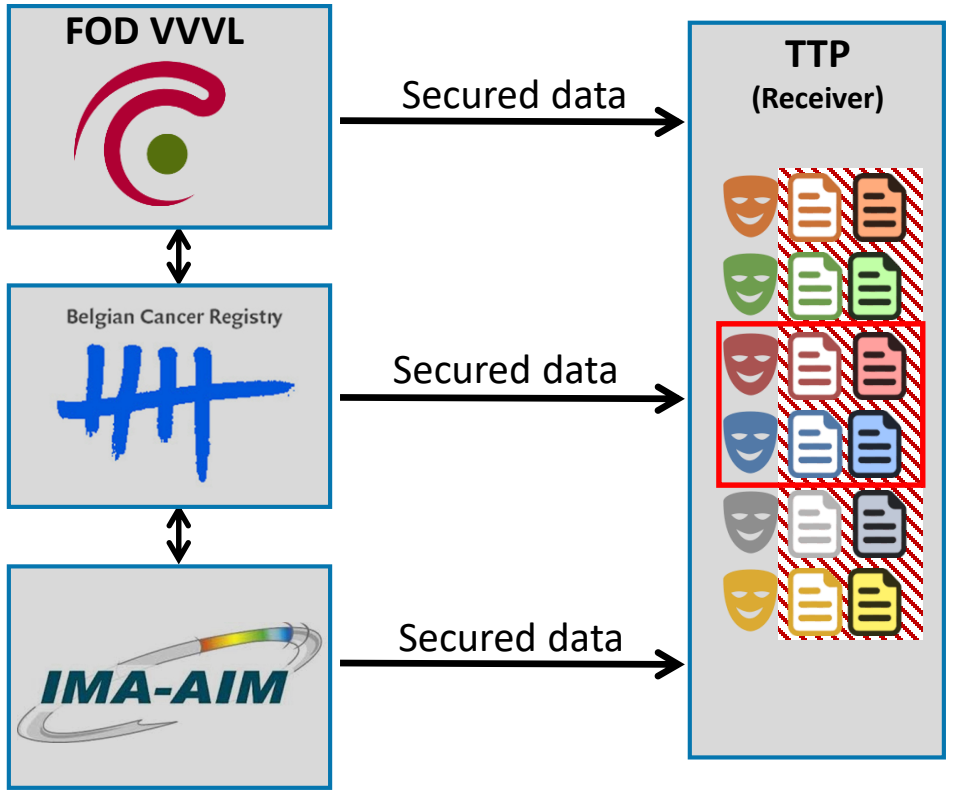
Eigenschappen

- Privacy-vriendelijk kruisen & pseudonimiseren
- Op uniforme & efficiënte wijze

3 stappen

1. Zenders maken onderling afspraken
2. Elke zender verstuurt alle potentieel relevante data geëncrypteerd & gepseudonimiseerd
3. Dankzij de afspraken tussen de zenders kan de ontvanger enkel de relevante records decrypteren





Zenders komen geen nieuwe (statistische of persoons-) gegevens te weten

Receiver komt enkel de minimum noodzakelijke gepseudonimiseerde **persoonsgevens** te weten.

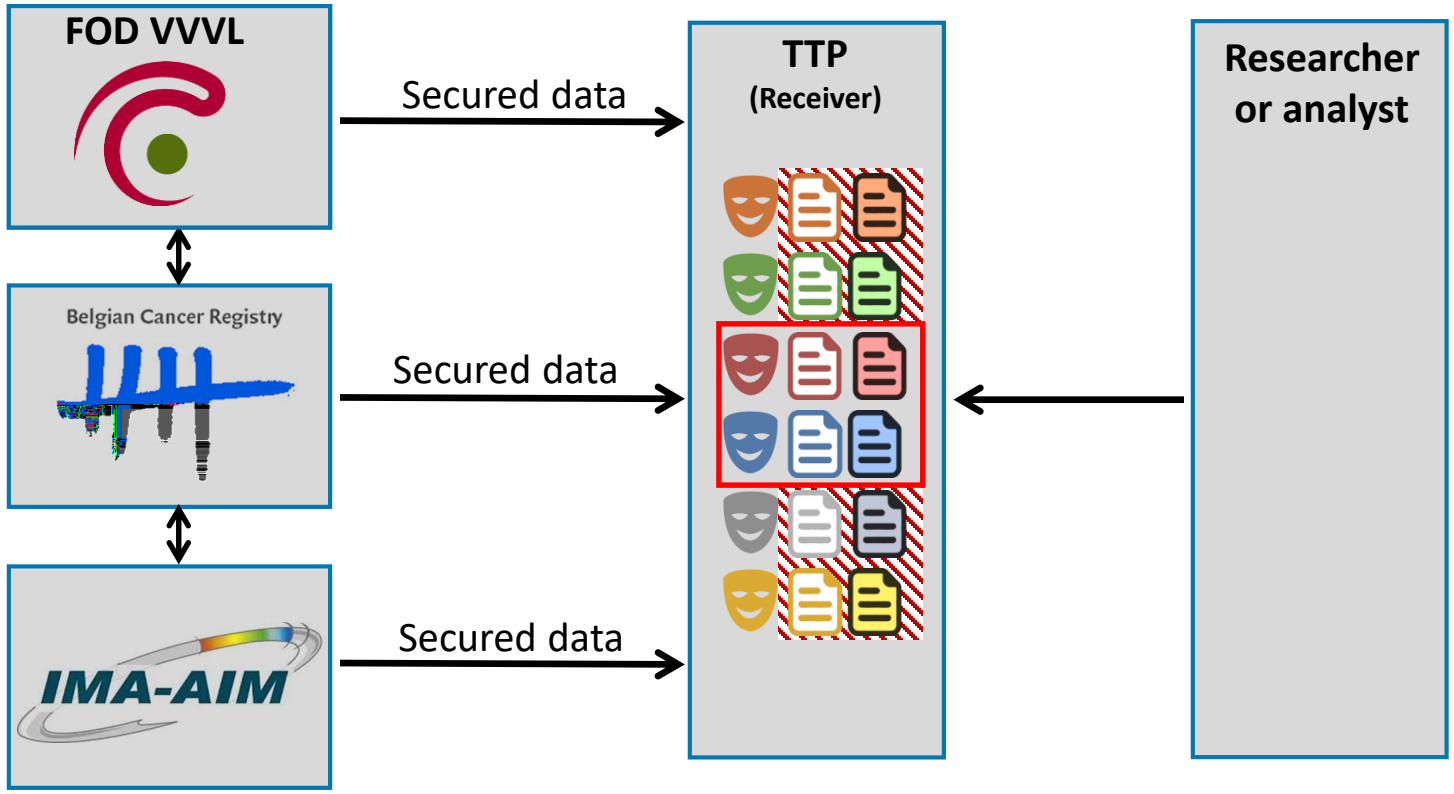
Minimale hoeveelheid **statistische data** lekt naar receiver
(in vb.: aantal burgers met kankerdiagnose)

Smals
ICT for society

Oblivious join - Concept

Taken TTP

- Verwijdert asap irrelevante cijferteksten
- Doet eventueel bijkomende controles op data
- Doet toegangscontrole op onderzoeker



Oblivous join – Validatie & code

Validatie concept

- Concept gevalideerd door KU Leuven
- KU Leuven heeft academische publicatie ingestuurd
  [Indien aanvaard] Sterke validatie door wereldwijde experts (peer review)

Applicatie

- Code Tussen PoC en PROD
- Grote testen succesvol
- Command line interface
- Demonstreerbaar (4 VMs)
- Geen integratie vereist

Use cases

- Ontwikkeld voor specifieke use case
- Toepassingen in andere context?

Smals ICT for society

KU LEUVEN

DEPARTMENT OF COMPUTER SCIENCE

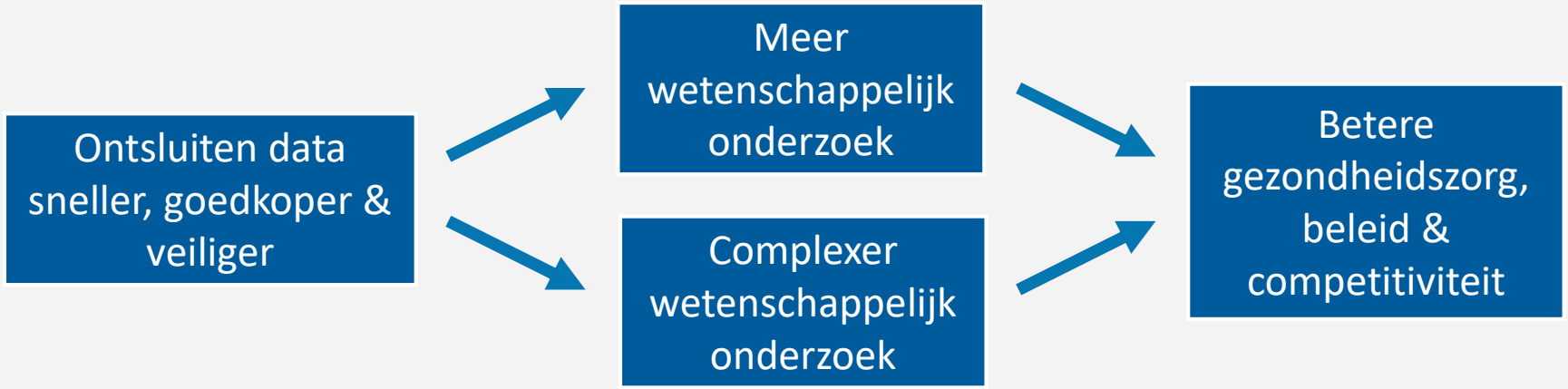
Kristof Verslype

Oblivious join – Meerwaarde

Komt tegemoet aan een reële behoefte

- Privacy-vriendelijk
- Uniforme, efficiënte werkwijze
- Niet-intrusief

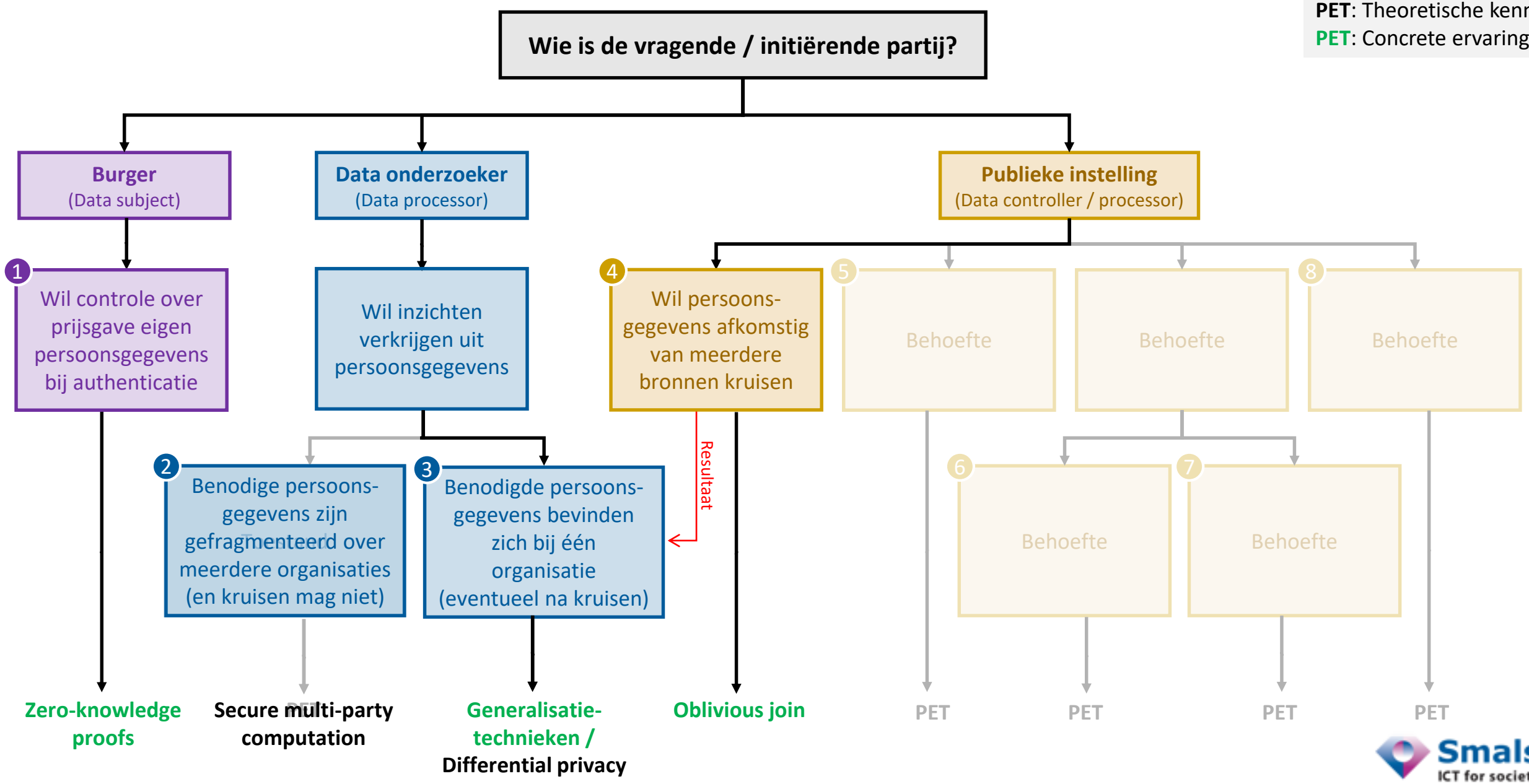
Opportuniteiten



Smals ICT for society

Selectieboom

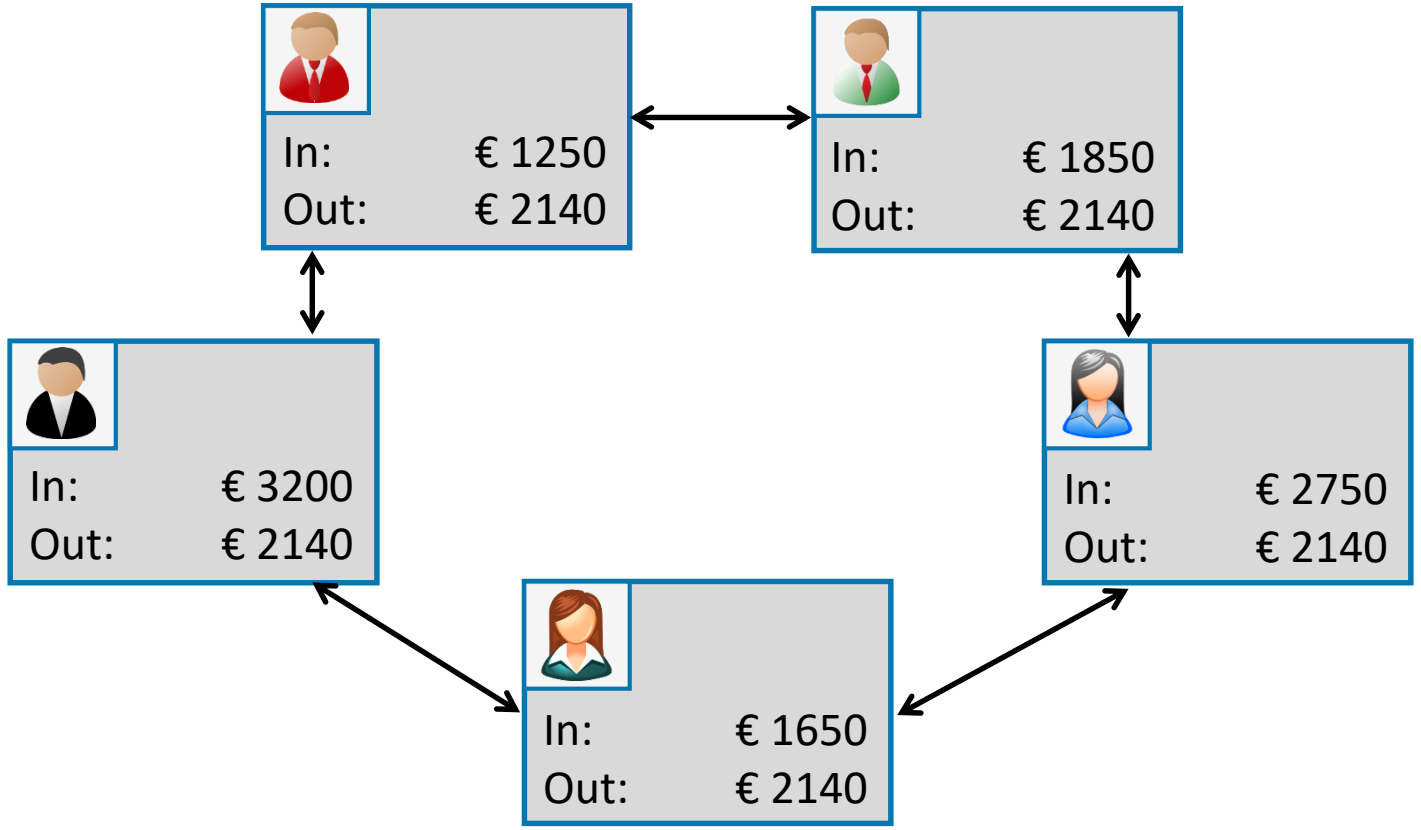
PET: Theoretische kennis
PET: Concrete ervaring



Secure Multiparty Computation (SMC)

Voorbeeld

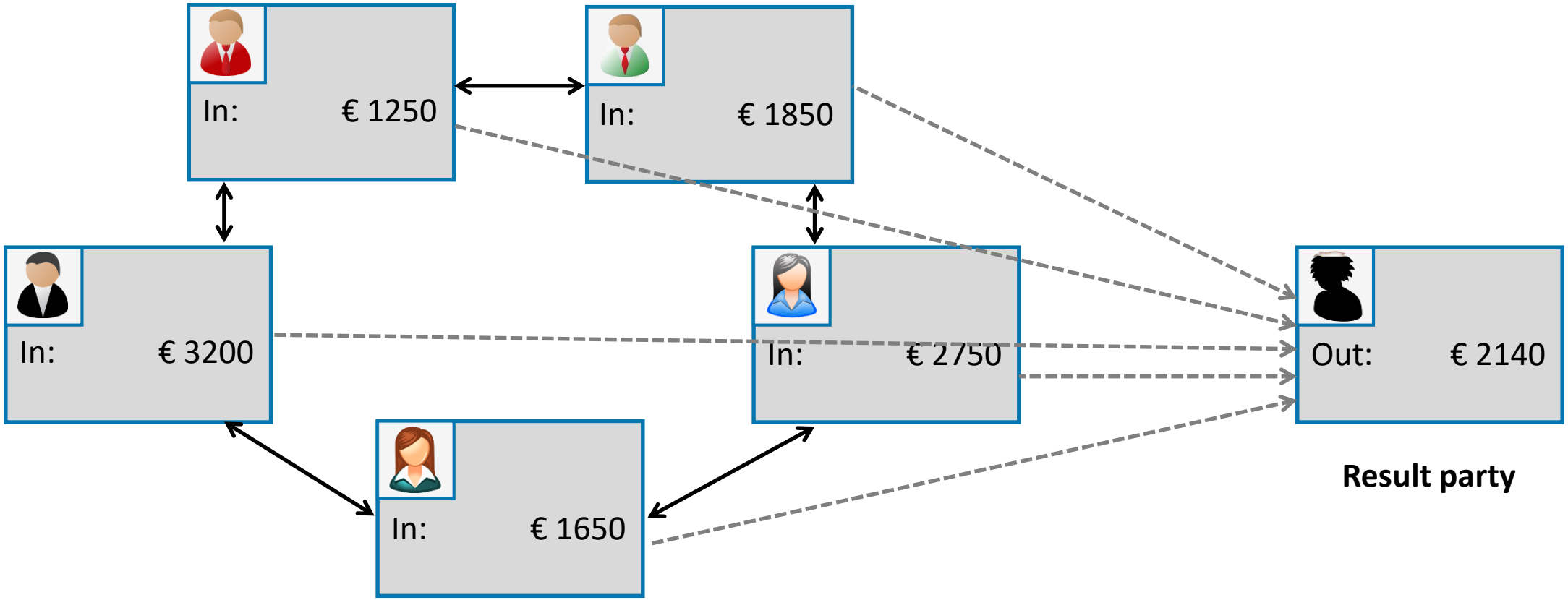
Berekenen gemiddelde loon, zonder individuele lonen prijs te geven



Veralgemeende probleemstelling

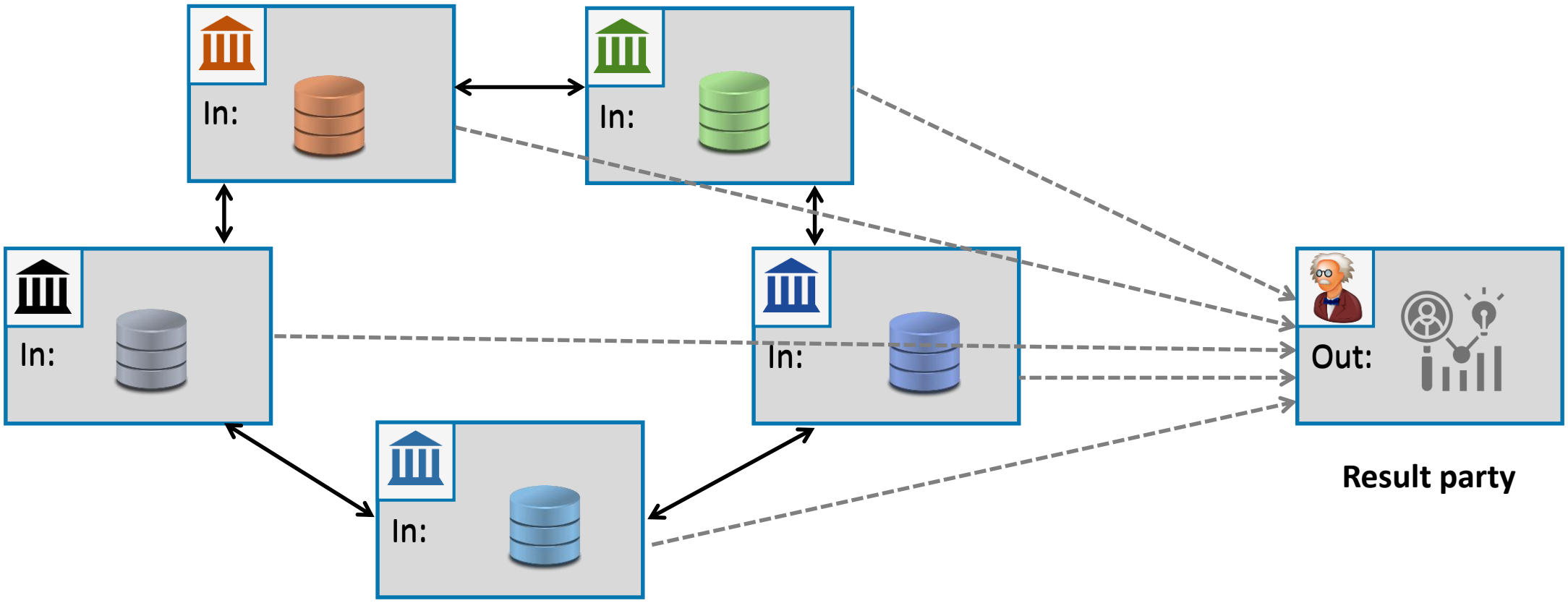
Kunnen we berekeningen collectief uitvoeren, dus zonder vertrouwde partij, waarbij meerdere participanten invoer aanleveren die toch confidentieel blijft?

Secure Multiparty Computation voor Analyse



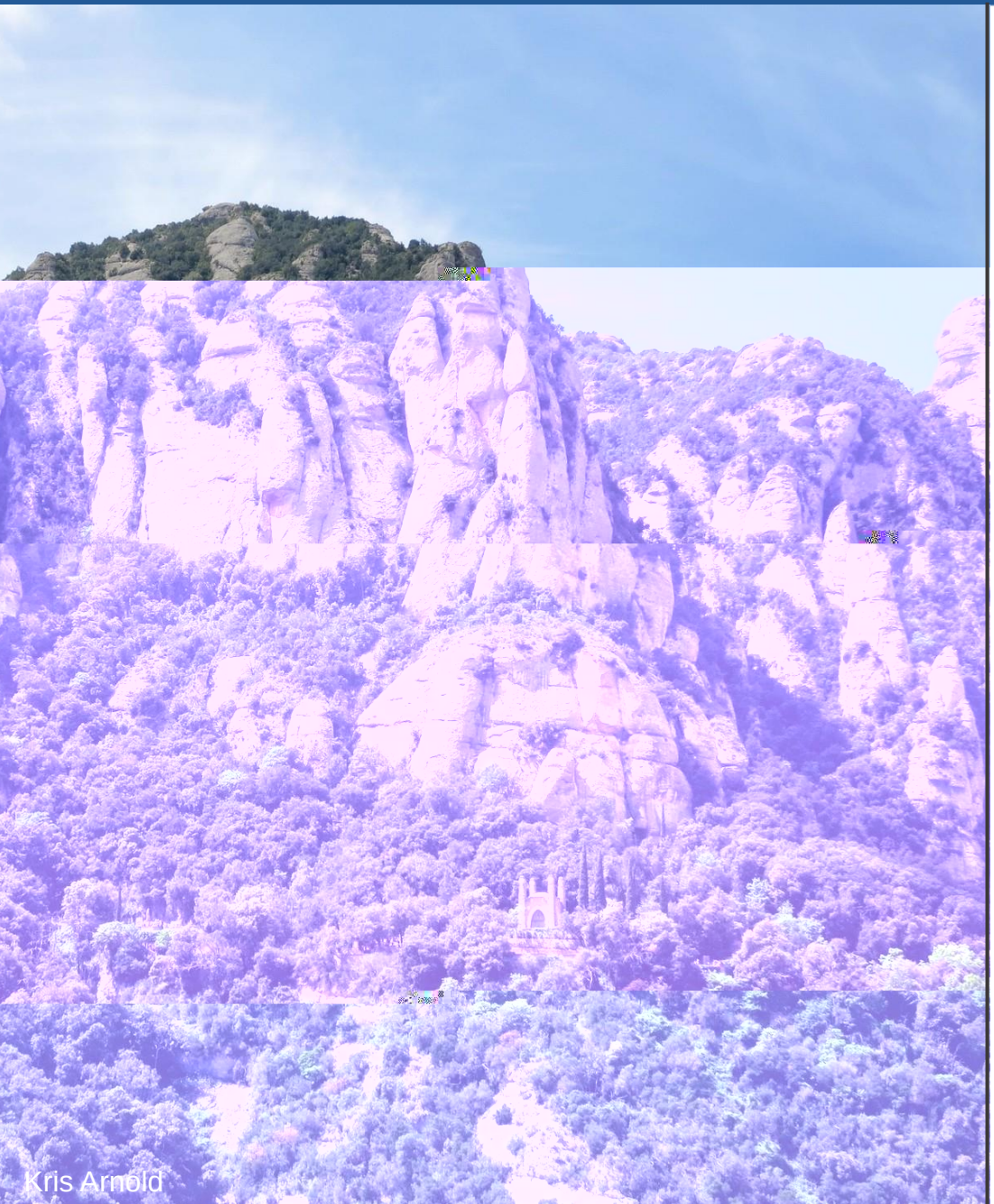
Computing parties = input parties

Secure Multiparty Computation voor Analyse



Computing parties = input parties

SMC voor analyse



Kris Arnold

Uitdagingen

- Onderzoeker kan niet langer data zelf bekijken
- Meerdere onafhankelijke partijen vereist **met voldoende technische know-how**
- Paar grootteordes trager + communication overhead

Commercialisatie

CYBERNETICA

RosemanLabs
PRIVACY BY DESIGN

Use case Estland
Verband opleiding & loon/belastingen

Evangelisatie-fase

Filosofie
Drie onafhankelijke entitiiteiten vormen samen virtueel, privacy-vriendelijk data warehouse

Smals
ICT for society

Nederlandse overheid experimenteert reeds

TNO innovation for life

Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek

*"Er zijn ontzettend veel toepassingsmogelijkheden voor privacyverbeterende technieken zoals SMC en FL [Federated Learning]. Zo kan de **effectiviteit van de zorg** vergroot worden door op een privacy vriendelijke manier inzichten uit patiëntdata te verkrijgen. De groeiende **financiële criminaliteit** kan ingedamd worden door het veilig koppelen van gevoelige data van verschillende financiële organisaties. Daarnaast kan de overheid haar **dienstverlening verbeteren** door privacy respecterende samenwerkingen tussen verschillende overheidsinstanties."*

https://publications.tno.nl/publication/34637924/c6SScX/TNO-2021-technologische.pdf

Smals ICT for society

SMC als gedistribueerde makelaar (broker)

Veiling

- In gebruik sinds 2009 voor suikerbieten
- Wordt uitgebreid (vb. elektriciteit)
- Dubbele veiling (verkopers & kopers bieden)
- Biedingen moeten confidentieel blijven

PARTISIA

Containervervoer

- Welke containers op welke boot?
- Rederijen willen verborgen houden hoeveel capaciteit ze vrij hebben (~ bereidheid tot prijsdalingen)
- Klant wil niet prijsgeven hoeveel hij bereid is te betalen (~ wanhoop)

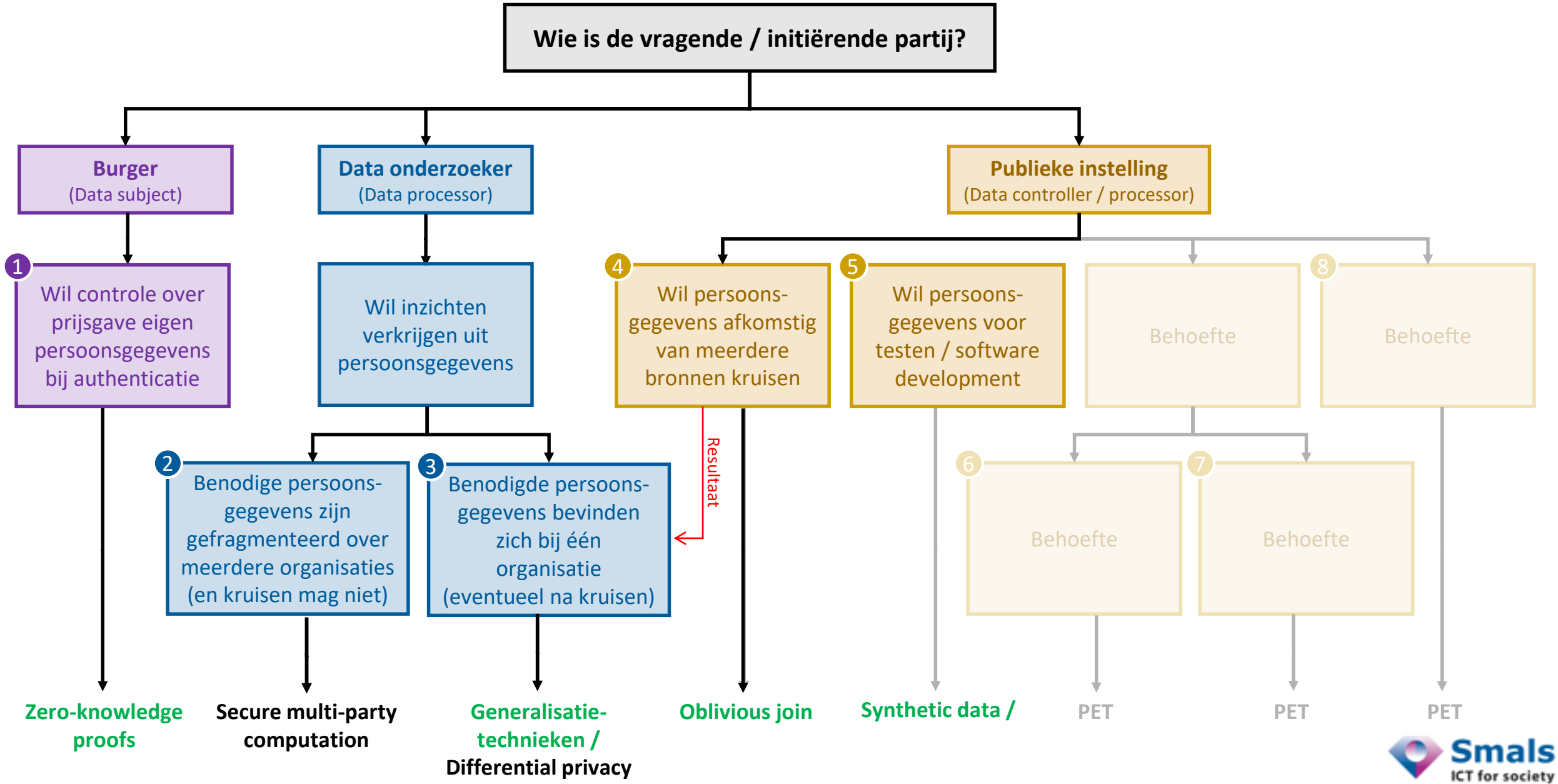
→ werk door SAP omstreeks 2000. Nooit live. Waarschijnlijk te vroeg

Dark pools

- 40% van alle aandelen wereldwijd via dark pools verhandeld
- Ontransparante bedrijven die vertrouwd moeten worden
- Kunnen handelen met voorkennis

→ KU Leuven + US investeringsbank: Dark pools → SMC

Selectieboom



Synthetic data

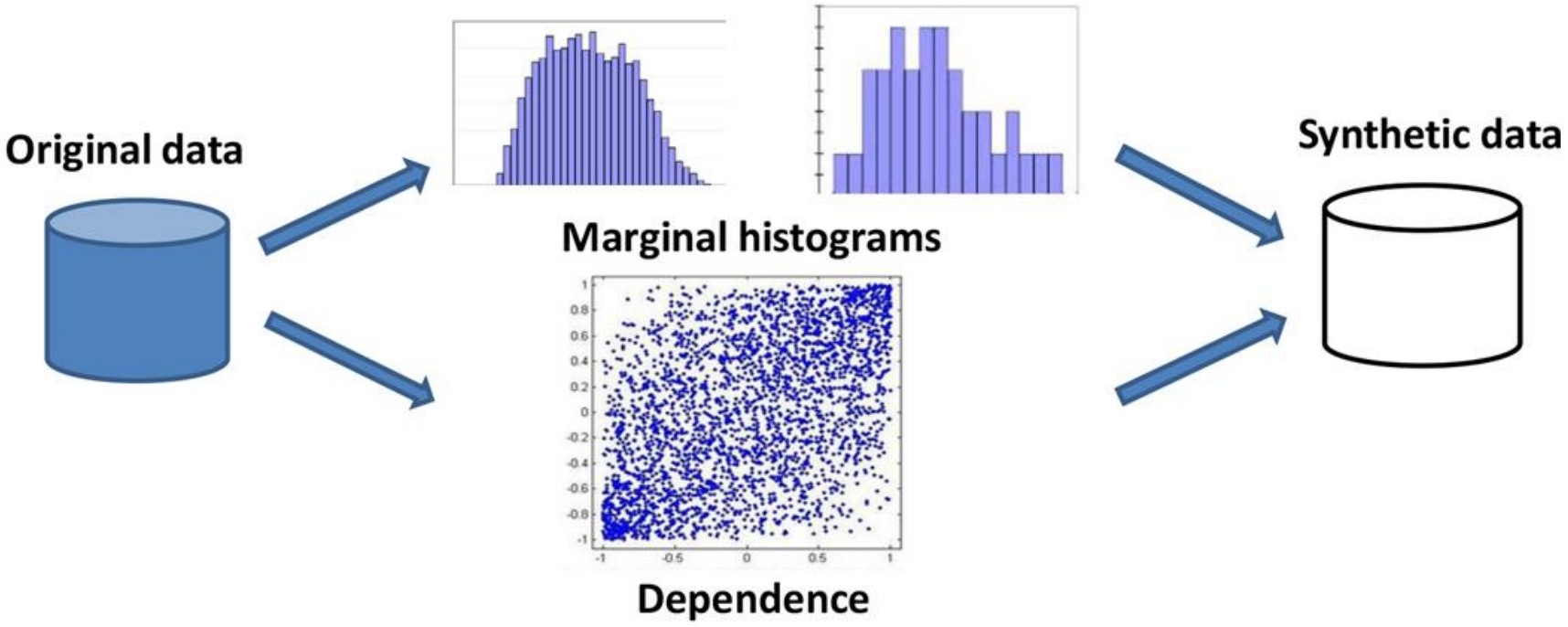
McGraw-Hill Dictionary

a N *NN*

a

Gebruik

Dataset met persoonsgegevens → Dataset met fake data met gelijkaardige statistische eigenschappen, maar met fake data (dus zonder persoonsgegevens)



→ Testen van software/scripts (vb. voor analyse), zonder privacyrisico's

Smals Research

Geteste producten

MOSTLY AI

- Commercieel
- Cloud
- User-friendly

SDV

The Synthetic Data Vault

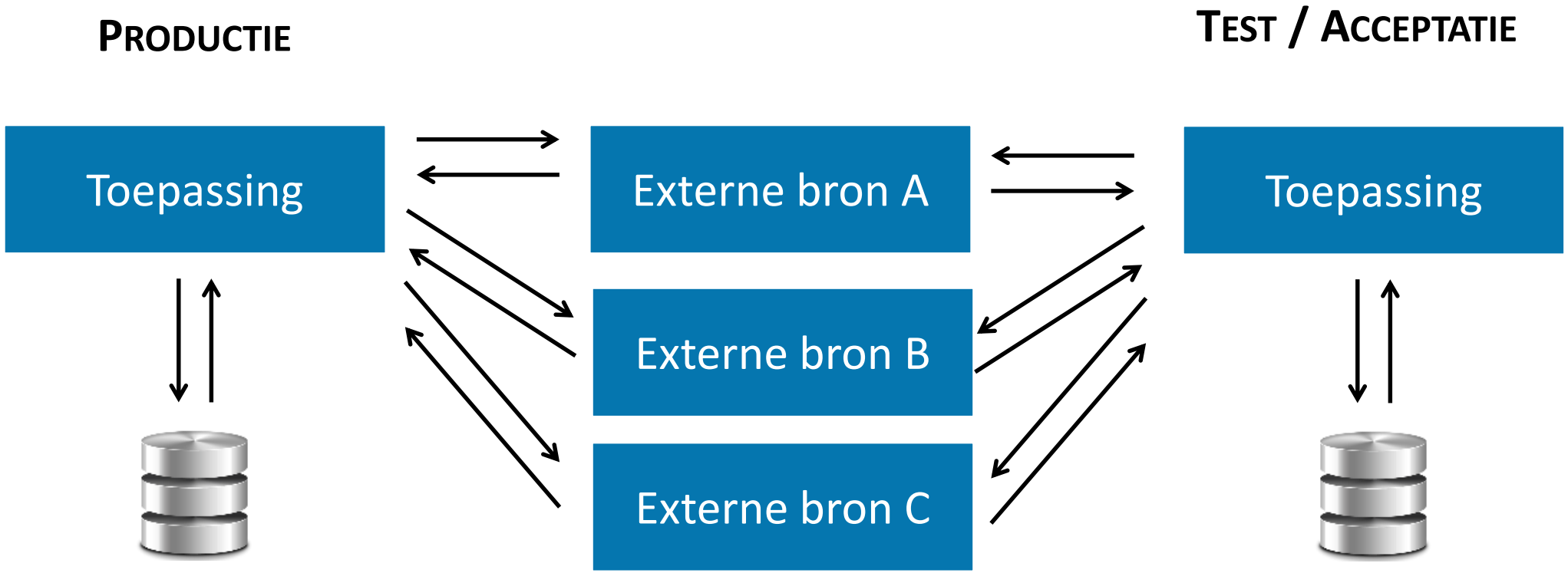
- Open source
- Python

Format-preserving encryption

Uitdaging

Vermijden identificeerbare persoonsgegevens in test & acc omgeving

Maar toch nog kunnen debuggen/testen



Probleem

Met Synthetic data inconsistenties tussen Test-toepassing en externe bronnen

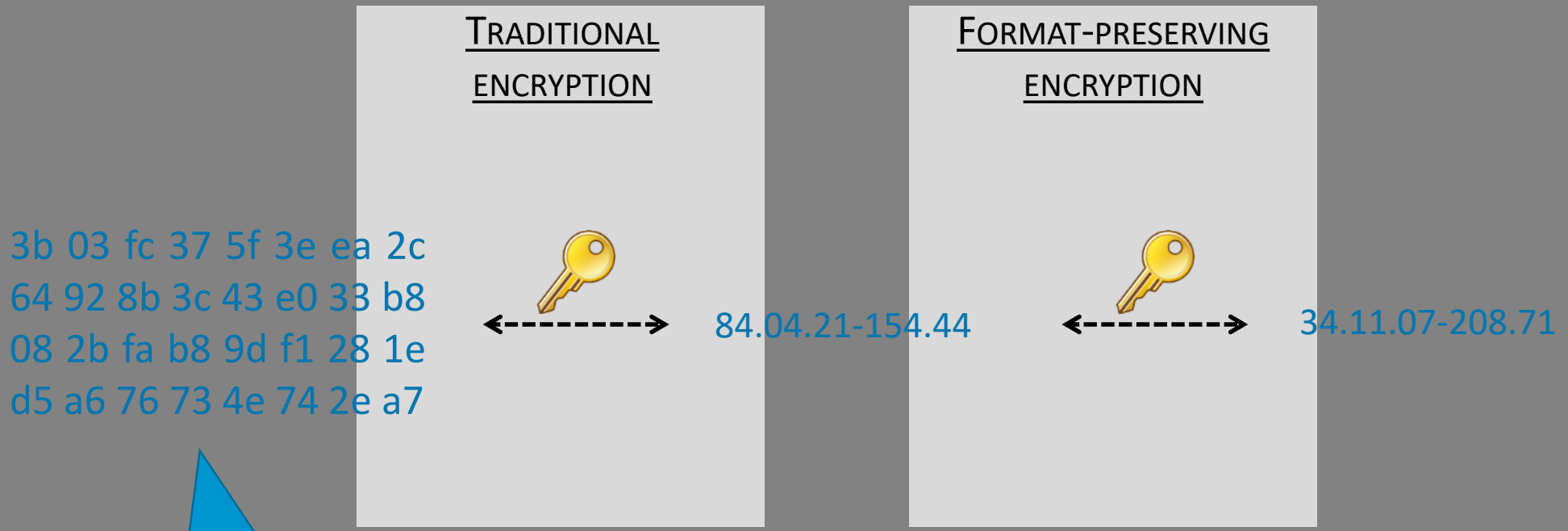
Vb. Test-toepassing wil informatie over niet bestaande burger

Smals ICT for society

Format-preserving encryption

Opzet

- Bewaren structuur / formaat van originele data na vercijfering
- [optioneel] bewaren informatie (vb. correcte checksum, geslacht, leeftijdscategorie)



Smals research

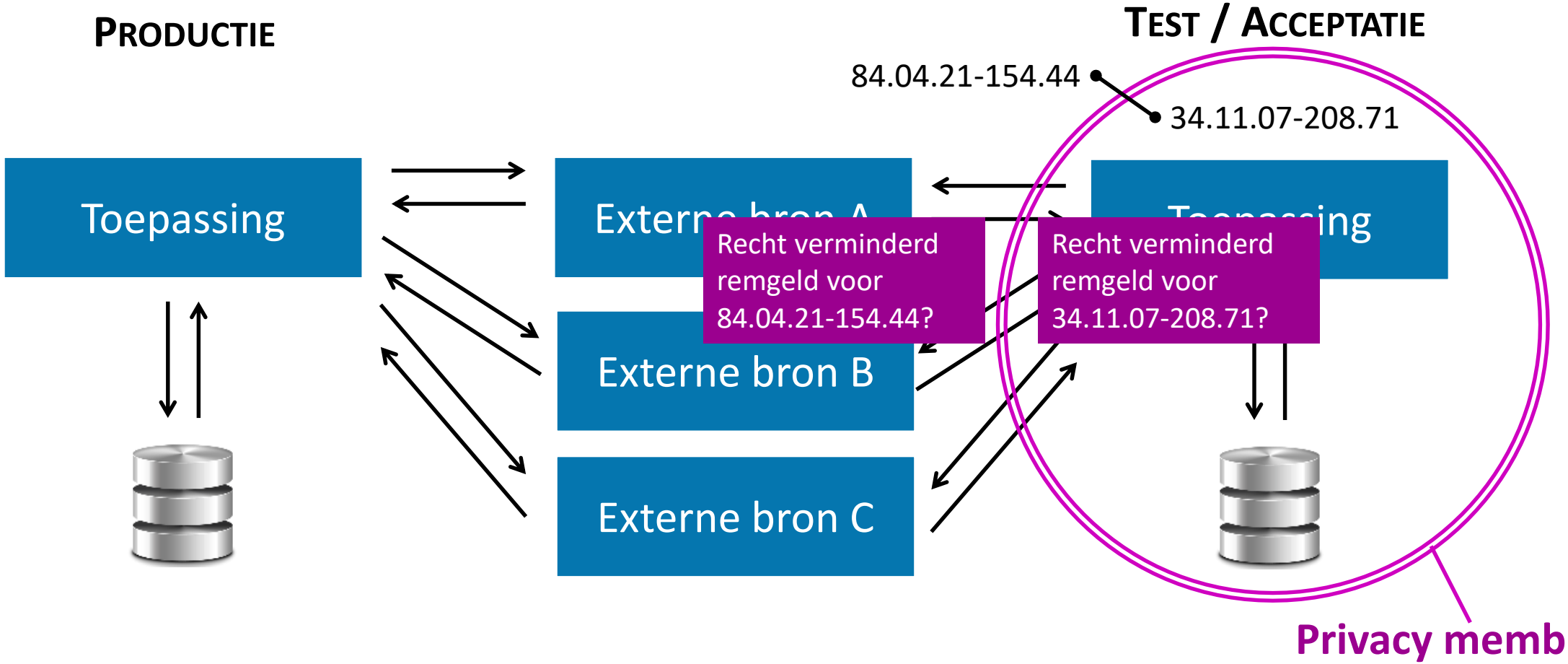
Heeft voor bestaande library ondersteuning voorzien voor rijksregisternummers

Format-preserving encryption

Uitdaging

Vermijden identificeerbare persoonsgegevens in test & acc omgeving

Maar toch nog kunnen debuggen/testen



Binnenkomende identifiers met FPE geëncrypteerd, uitgaande gedecrypteerd

(credits: K. Verslype & K. Maekelberghe)

Geen perfecte privacy, maar wel waardevol hulpmiddel

Publieke instelling wil systemen testen

Synthetic data

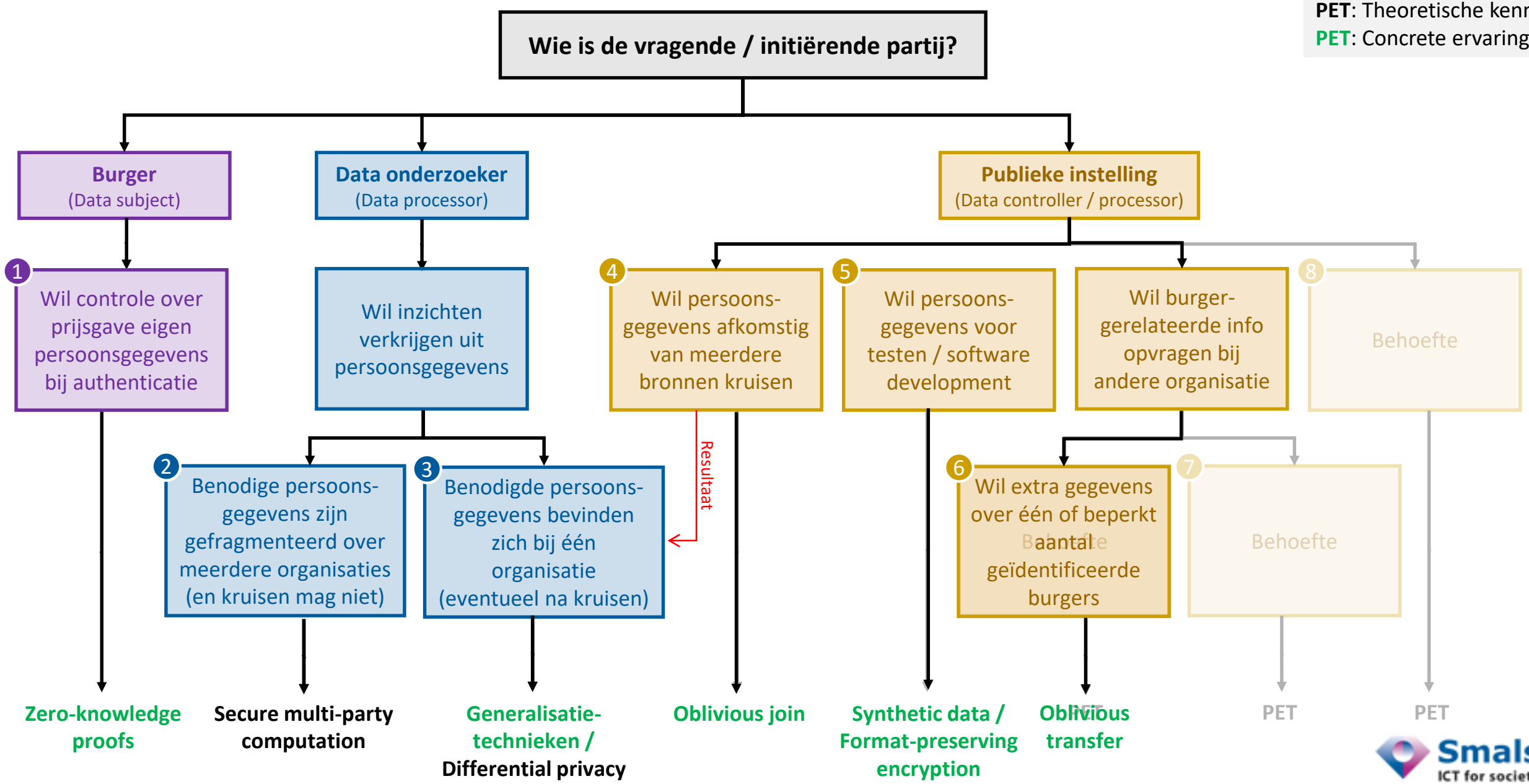
Format-preserving encryption

Kunnen privacy van de burger verbeteren voor testen van IT oplossingen (weliswaar voor verschillende use cases)

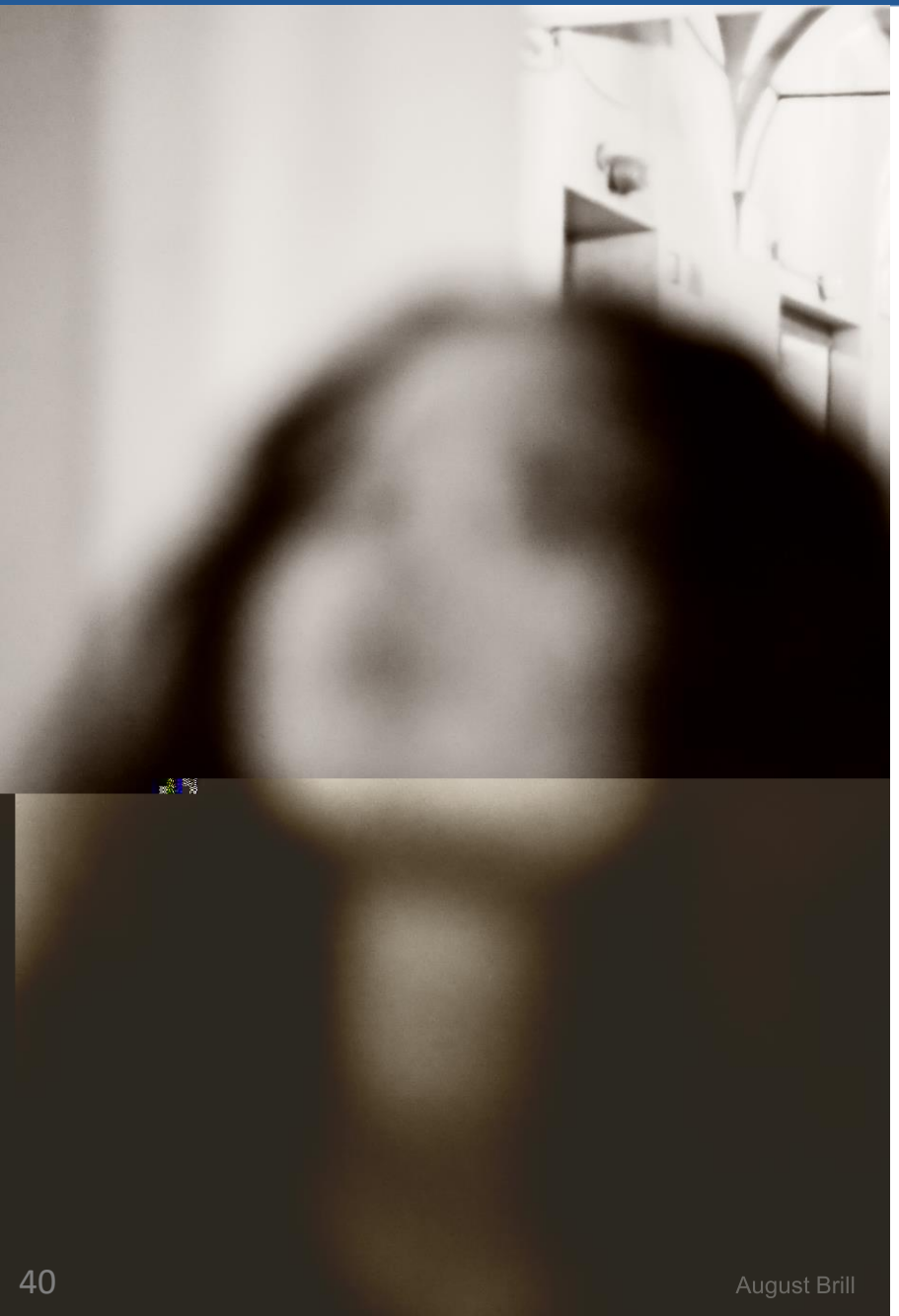
Smals ICT for society

Selectieboom

PET: Theoretische kennis
PET: Concrete ervaring

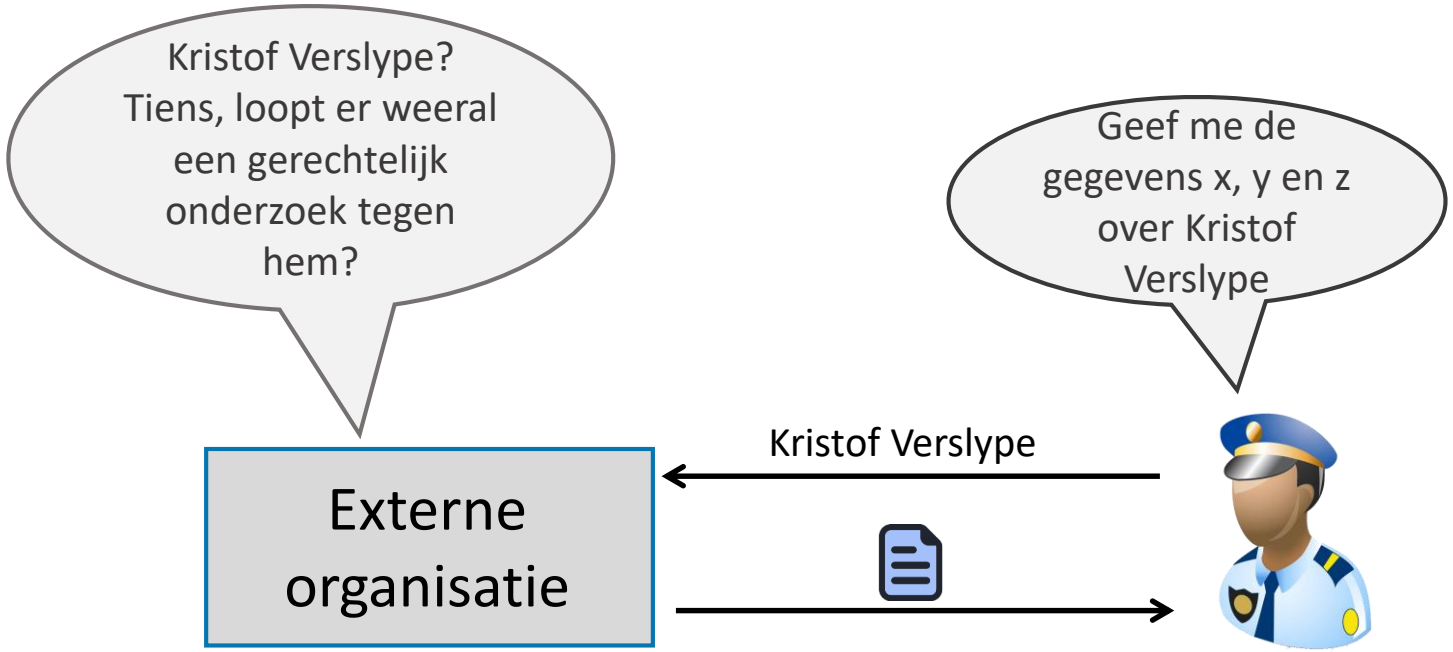


Oblivious transfer - Probleemstelling



Scenario / probleemstelling

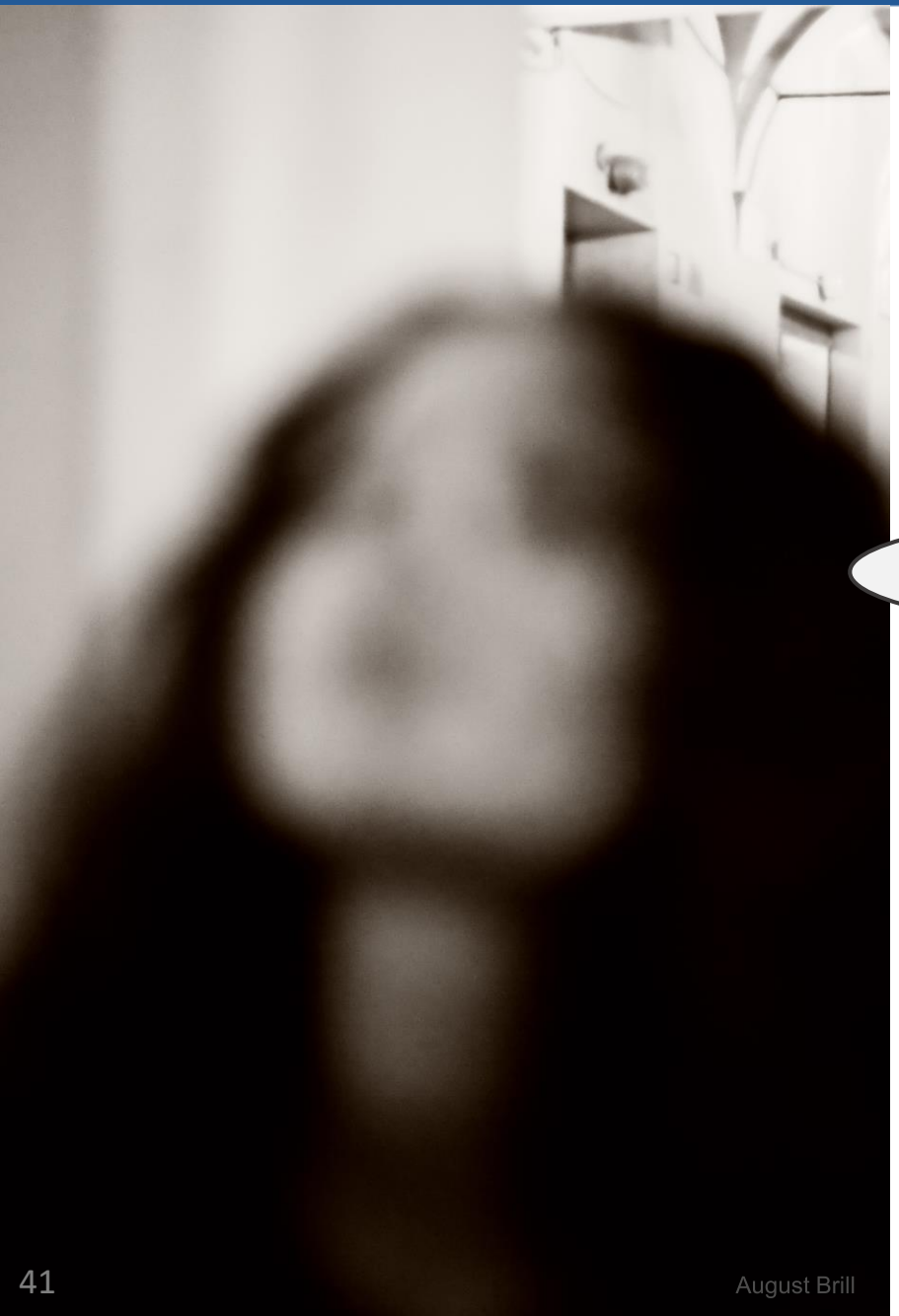
Onderzoek vanuit justitie naar een specifieke burger



Observatie

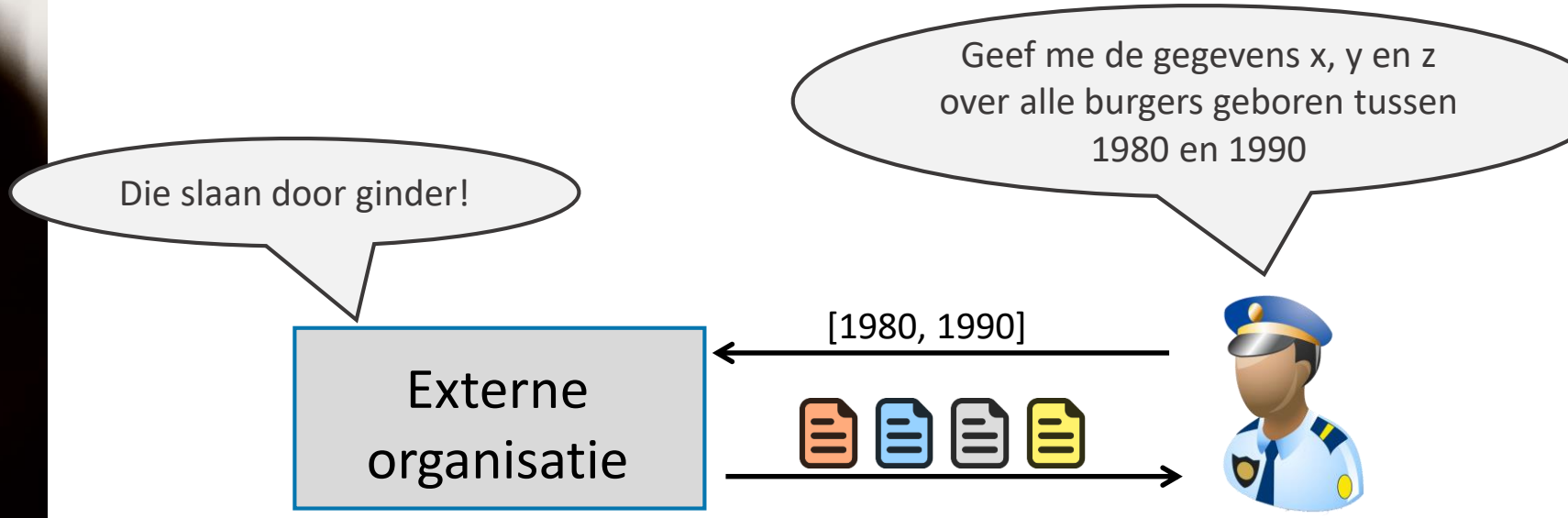
- Er wordt voldaan aan de informatievereiste
- Ten koste van privacy burger & confidentialiteit van het onderzoek

Oblivious transfer - Probleemstelling



Scenario / probleemstelling

Onderzoek vanuit justitie naar een specifieke burger



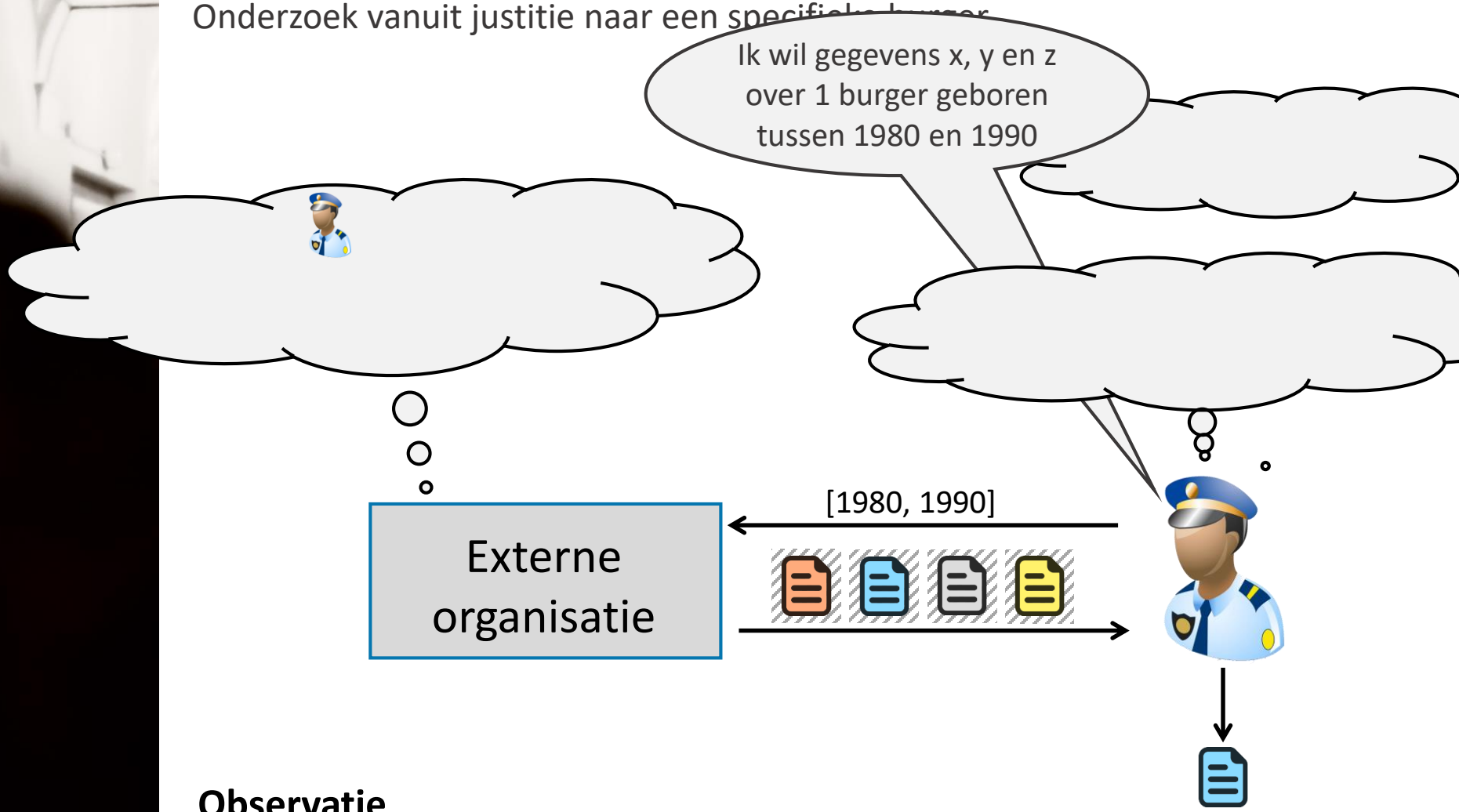
Observatie

- Disproportionele verwerking persoonsgegevens door justitie

Oblivious transfer - Probleemstelling

Scenario / probleemstelling

Onderzoek vanuit justitie naar een specifieke burger



Observatie

- Er wordt voldaan aan de informatievereiste
- Privacy burger & confidentialiteit van het onderzoek beschermd
- Geen TTP

Oblivious transfer - Conclusie

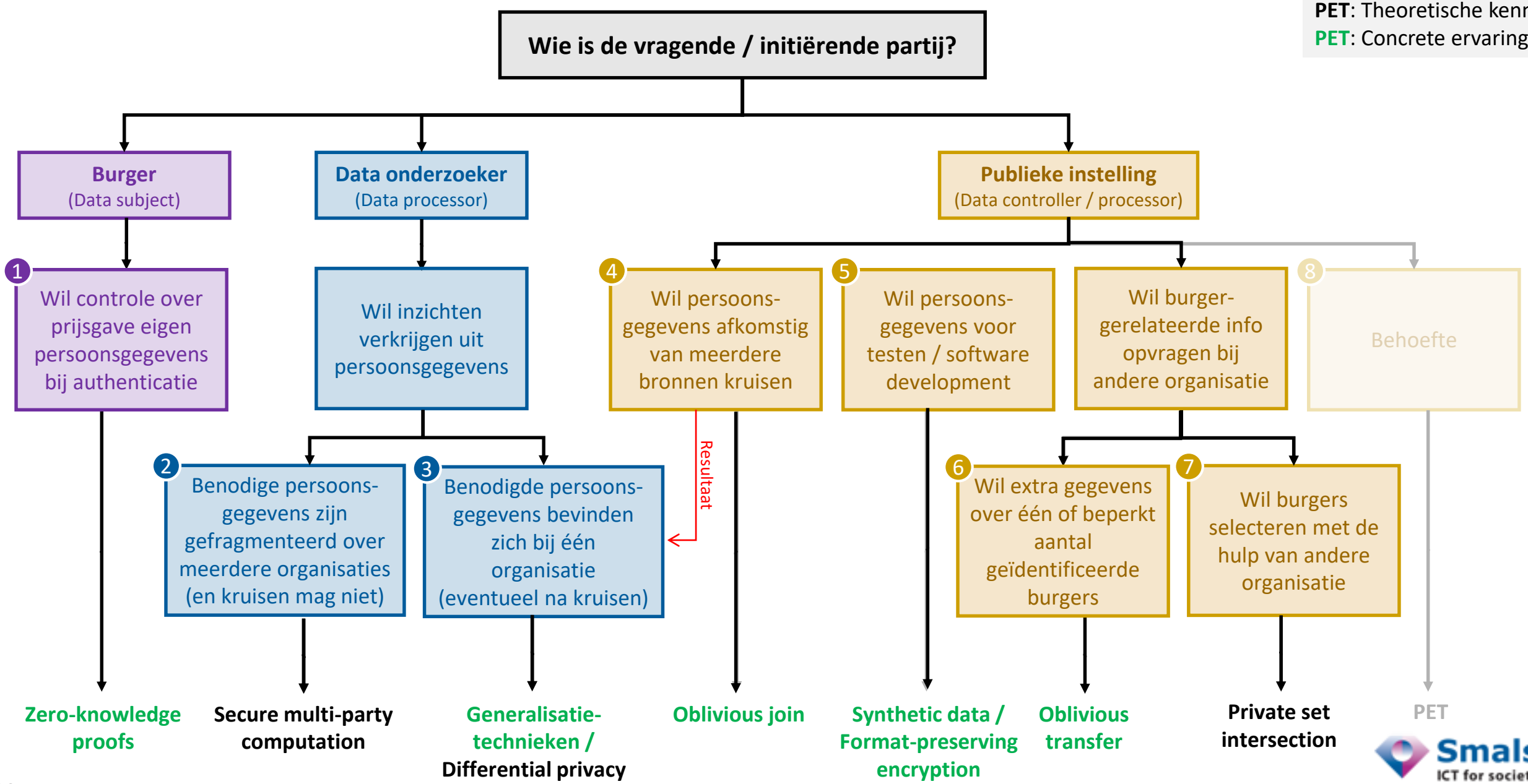
Oblivious transfer laat toe om informatie over een burger op te vragen zonder prijs te geven over wie het gaat

Smals Research

- Schreef Java library op basis bestaande wetenschappelijke publicaties
- Deed performantietesten
  Resultaat positief

Selectieboom

PET: Theoretische kennis
PET: Concrete ervaring



Private set intersection (PSI) - Probleemstelling

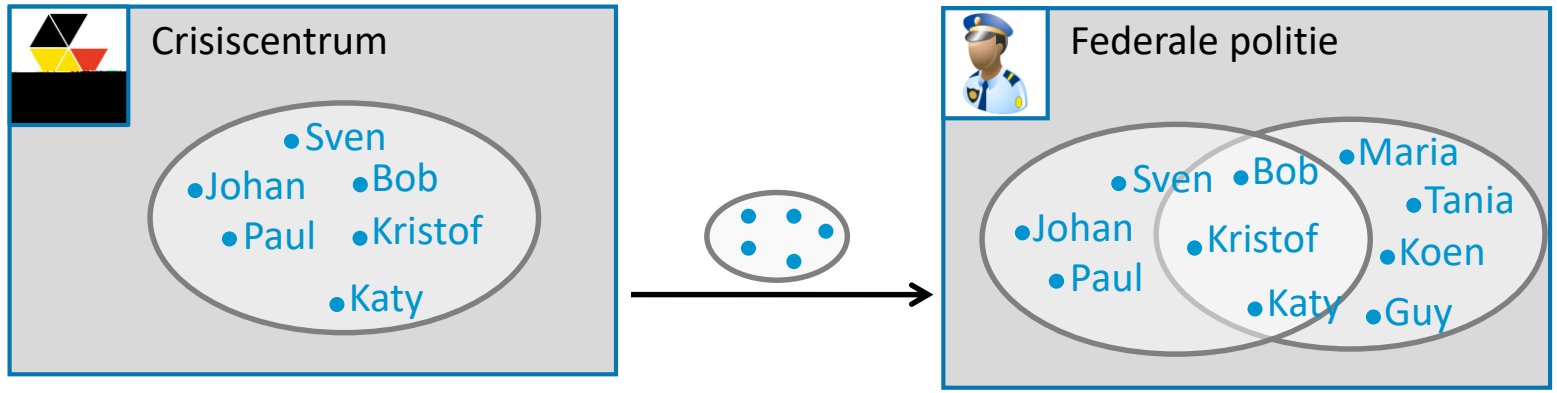
Mogelijke toepassing binnen publieke sector

Dossiers over zelfde burgers

Publieke dienst A wil weten over welke burgers ook publieke dienst B een dossier heeft

Fictief voorbeeld

Federale politie volgt een aantal burgers en wil weten wie daarvan door het crisiscentrum met hoge prioriteit gevolgd wordt.



Observatie

Onbedoelde prijsgave (lekkage) van informatie door Crisiscentrum aan Federale Politie

Private set intersection (PSI) - Probleemstelling

Mogelijke toepassing binnen publieke sector

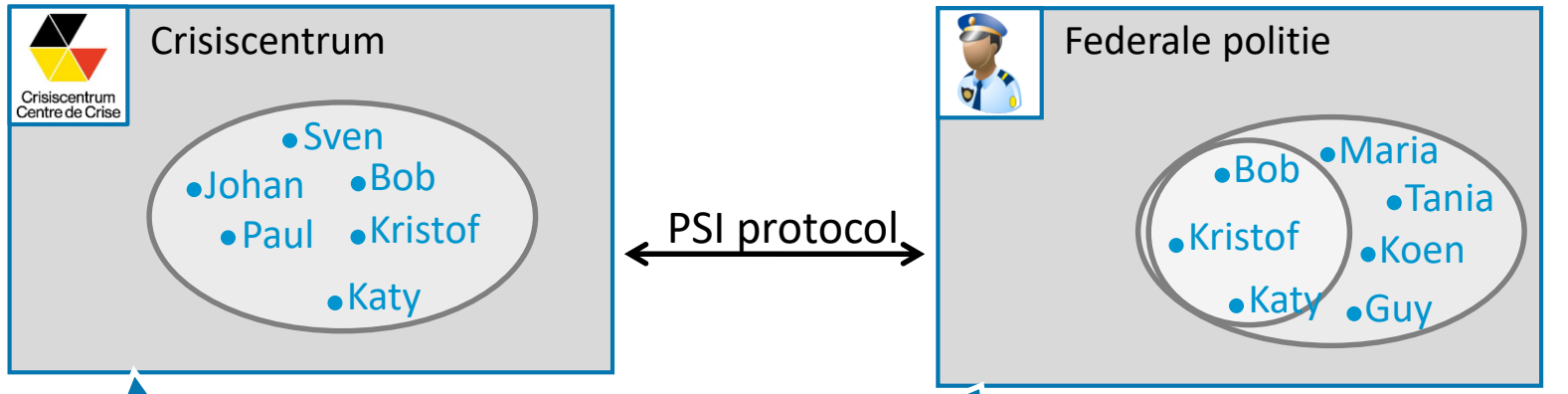
Dossiers over zelfde burgers

Publieke dienst A wil weten over welke burgers ook publieke dienst B een dossier heeft

- Wetshandhaving
- Achterstallige bijdragen bedrijven
- Verzekerd bij twee mutualiteiten?
- …

Fictief voorbeeld

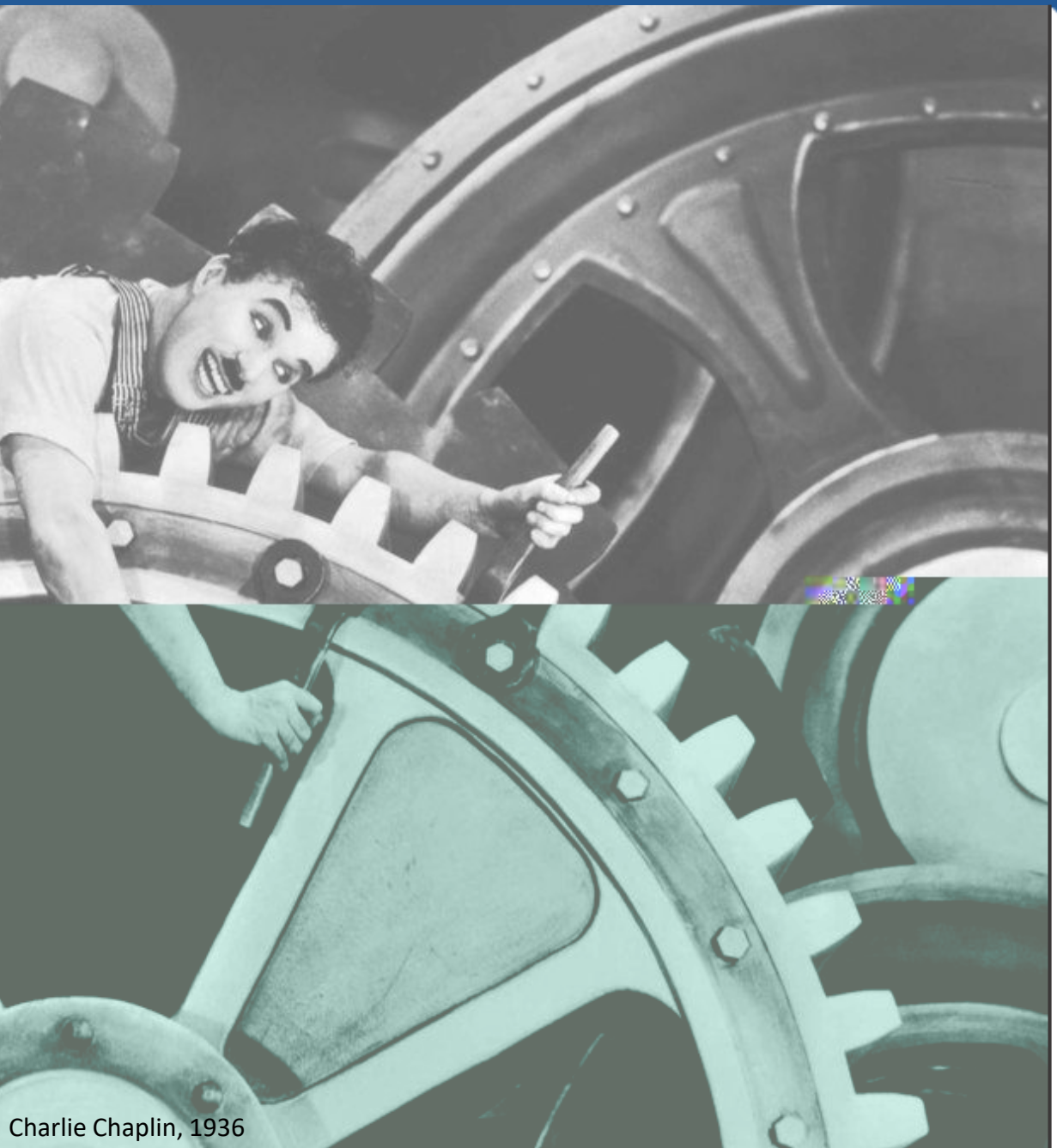
Federale politie volgt aan aantal burgers en wil weten wie daarvan door het crisiscentrum met hoge prioriteit gevolgd wordt.



Leert enkel dat er protocoluitvoering was met Federale Politie

- Komt enkel te weten voor welke individuen beide organisaties een dossier hebben
- Komt niet te weten over welke andere personen het crisiscentrum een dossier heeft

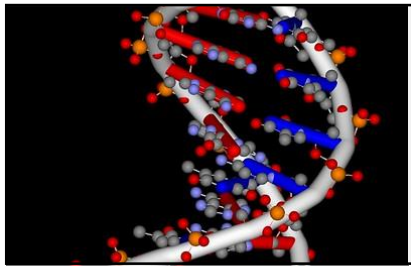
Private Set Intersection – Andere toepassingen



Charlie Chaplin, 1936

Soms verrassende toepassingen

Onveilig paswoord?
Is paswoord in online DB van gelekte paswoorden?
In Google Chrome vanaf v.79



Erfelijke ziektes
Wat is de doorsnede van mijn DNA sequenties en die van erfelijke ziektes in online DB?

Private contact discovery
Wie van mijn contacten heeft ook een account op messaging platform?

Smals
ICT for society

Private Set Intersection - Conclusie

Samengevat

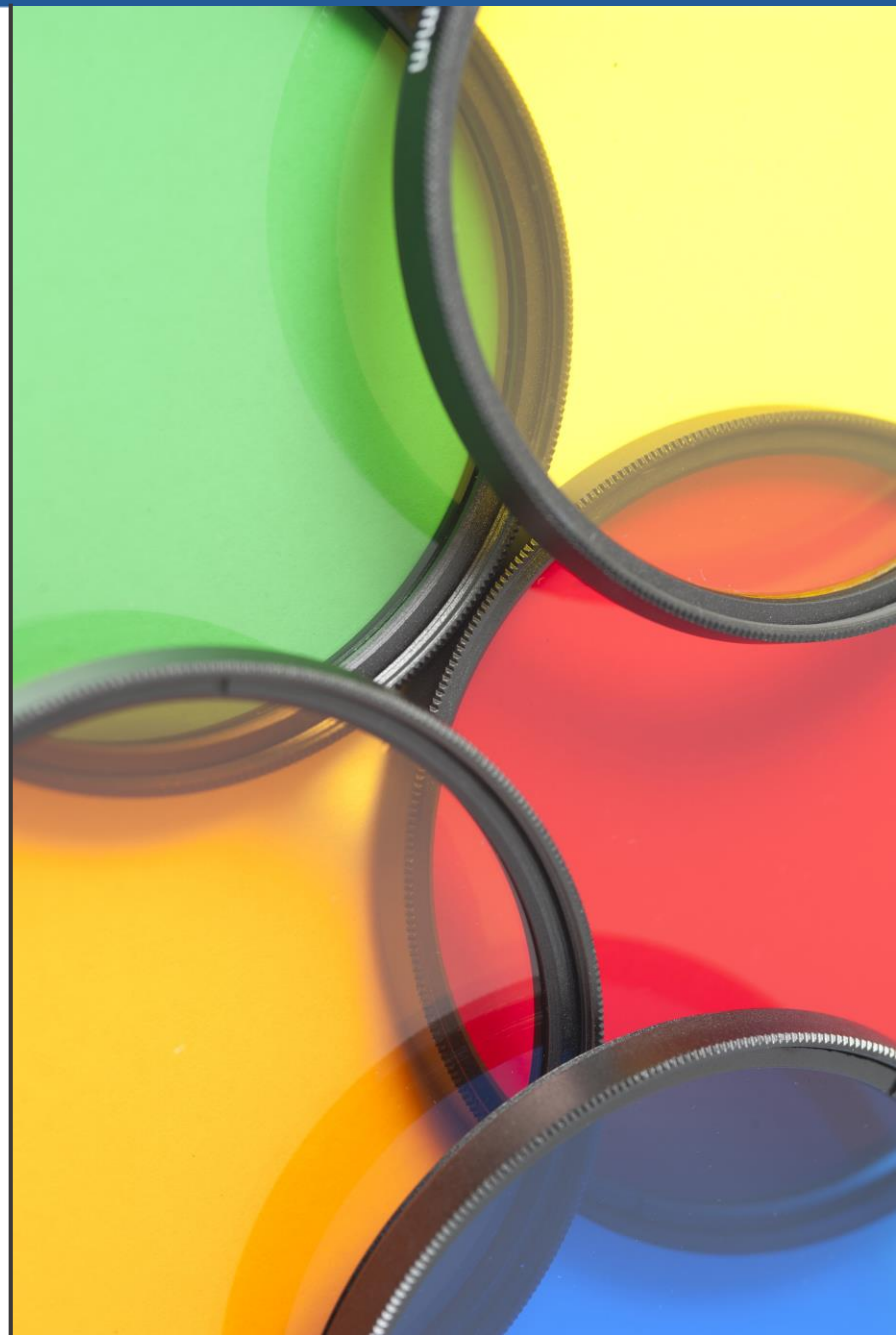
- Conceptueel relatief eenvoudig
- Interessante use cases
- Wordt in de praktijk gebruikt

Code

- Open source libraries beschikbaar op Github (te testen)

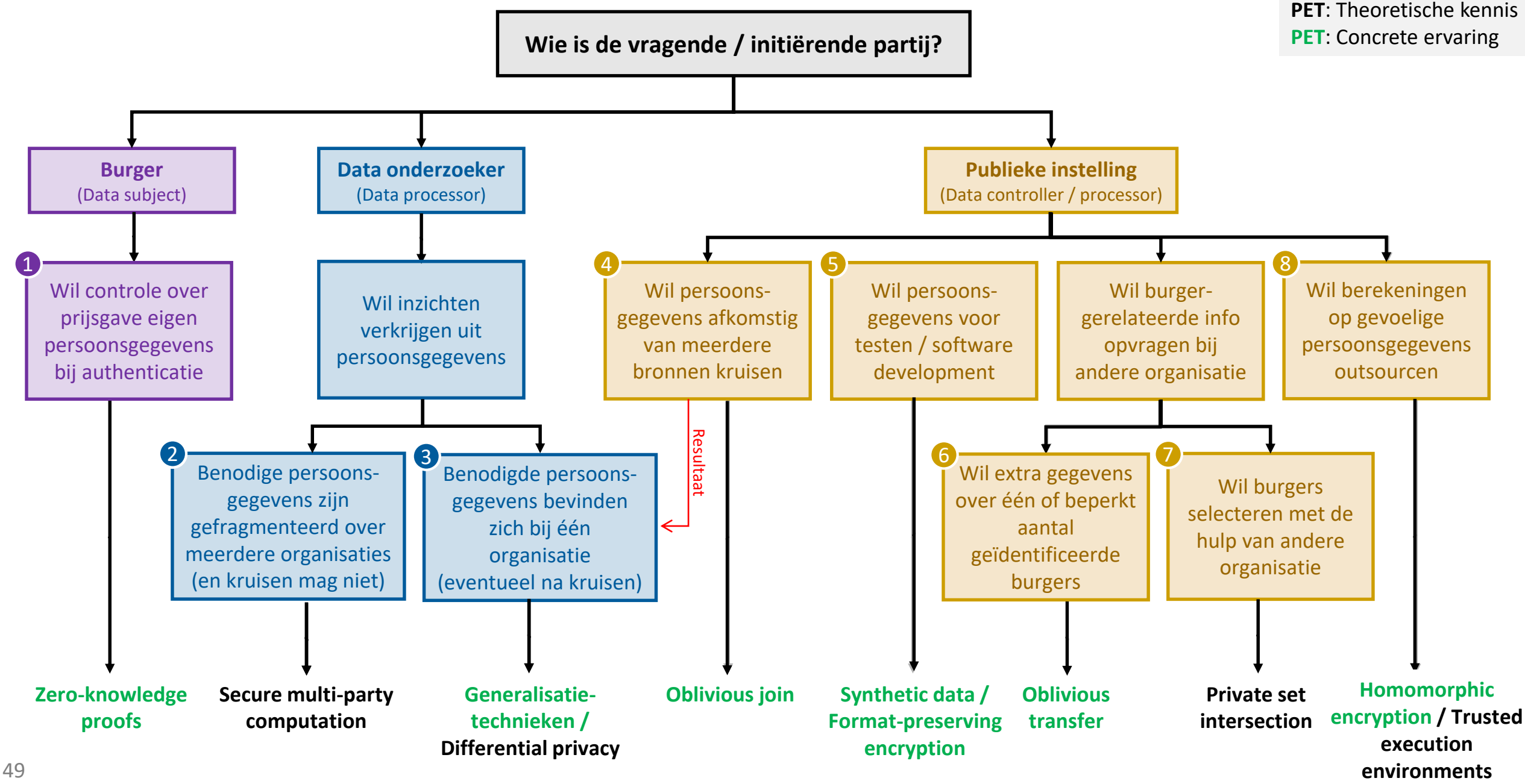
Variaties

- **Private Set Intersection Cardinality (PSI-CA)**
  Niet de elementen in de doorsnede maar enkel het aantal elementen wordt prijsgegeven
- **Multiparty Private Set Intersection**
  Meer dan 2 partijen betrokken in protocol



Selectieboom

PET: Theoretische kennis
PET: Concrete ervaring



Outsourcen berekeningen

Gartner

a N

NN

N *a*

N

Source

N

aN

a *N*

N

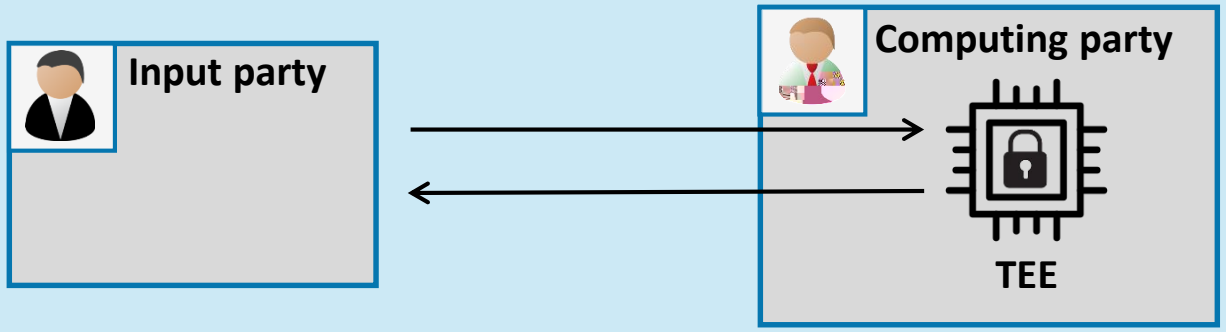
N

aN

Publieke instelling

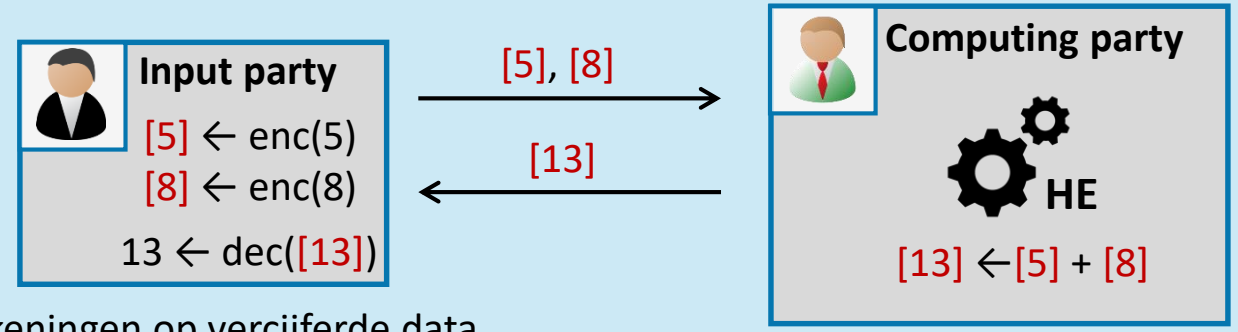
- Wil gebruik maken van cloud omgevingen buiten haar controle
- Wil niet dat cloud providers (=computing party) toegang heeft tot de persoonsgegevens

Trusted Execution Environment (TEE)



Berekeningen m.b.v. gespecialiseerde hardware, in aparte enclave.

Homomorfe Encryptie (HE)

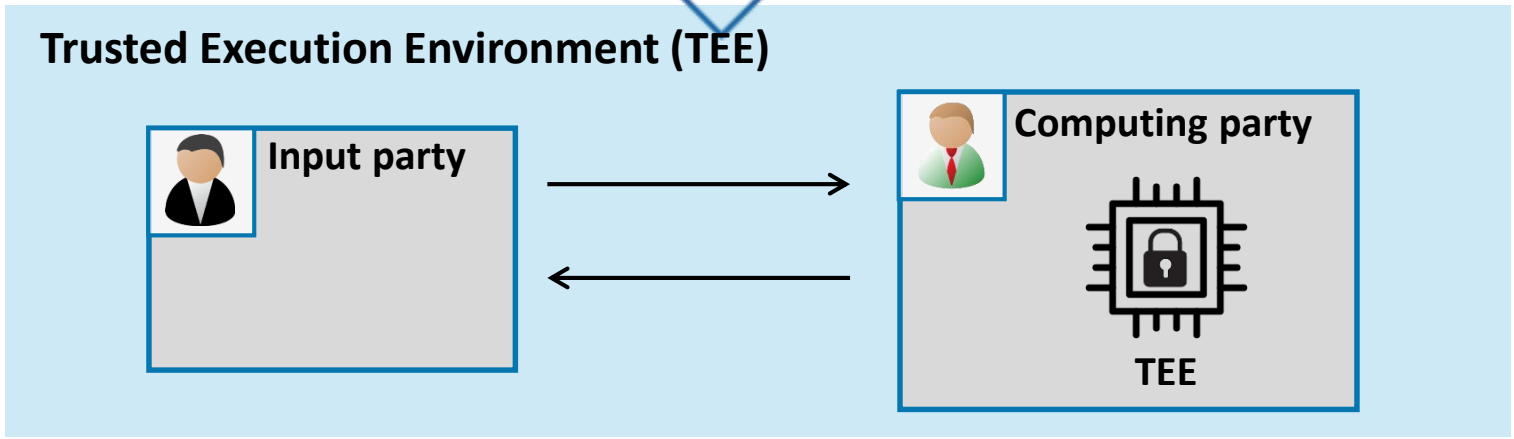


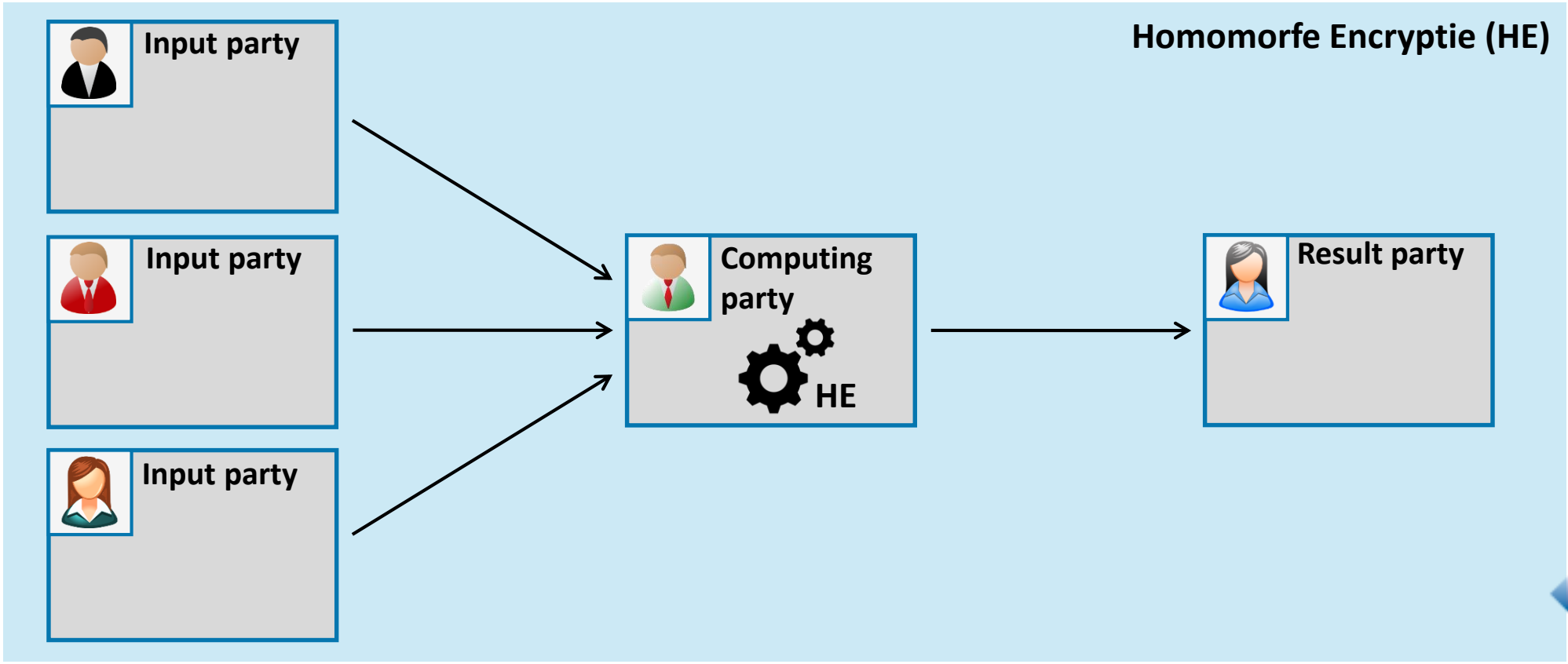
Berekeningen op vercijferde data

5 Onvercijferd
[5] Vercijferd

Smals ICT for society

Outsourcen berekeningen





Outsourcen berekeningen

	Trusted Execution Environment (TEE)	Homomorfe Encryptie (HE)
Beveiligd door	Gespecialiseerde hardware	Cryptografie (=wiskunde)
Efficiëntie	Hoog	- HE <<< SMC <<< traditioneel - Hang sterk af van vereiste operaties
Input parties	1	1 of meerdere
Vertrouwen in computing party	Onvermijdelijk gevoelig voor side-channel attacks. Geen gekende cases, maar voldoende bewijs dat het kan. (MicroScope, Plundervolt, SGAxe) *a* *N* *a* *a* Prof. Nigel Smart, COSIC, KU Leuven. TEEs prima wanneer zelf controle over toestel of als secundaire beveiliging	- Mag niet samenspannen met decrypterende partij - Ziet data niet, maar moet wel vetrouwd worden om berekeningen correct uit te voeren. (ofwel *N*)
Voorbeelden	Intel SGX, ARM TrustZone	**Microsoft SEAL**, IBM Helib, PALISADE (allen open source)

Outsourcen berekeningen

Daniel Spiess

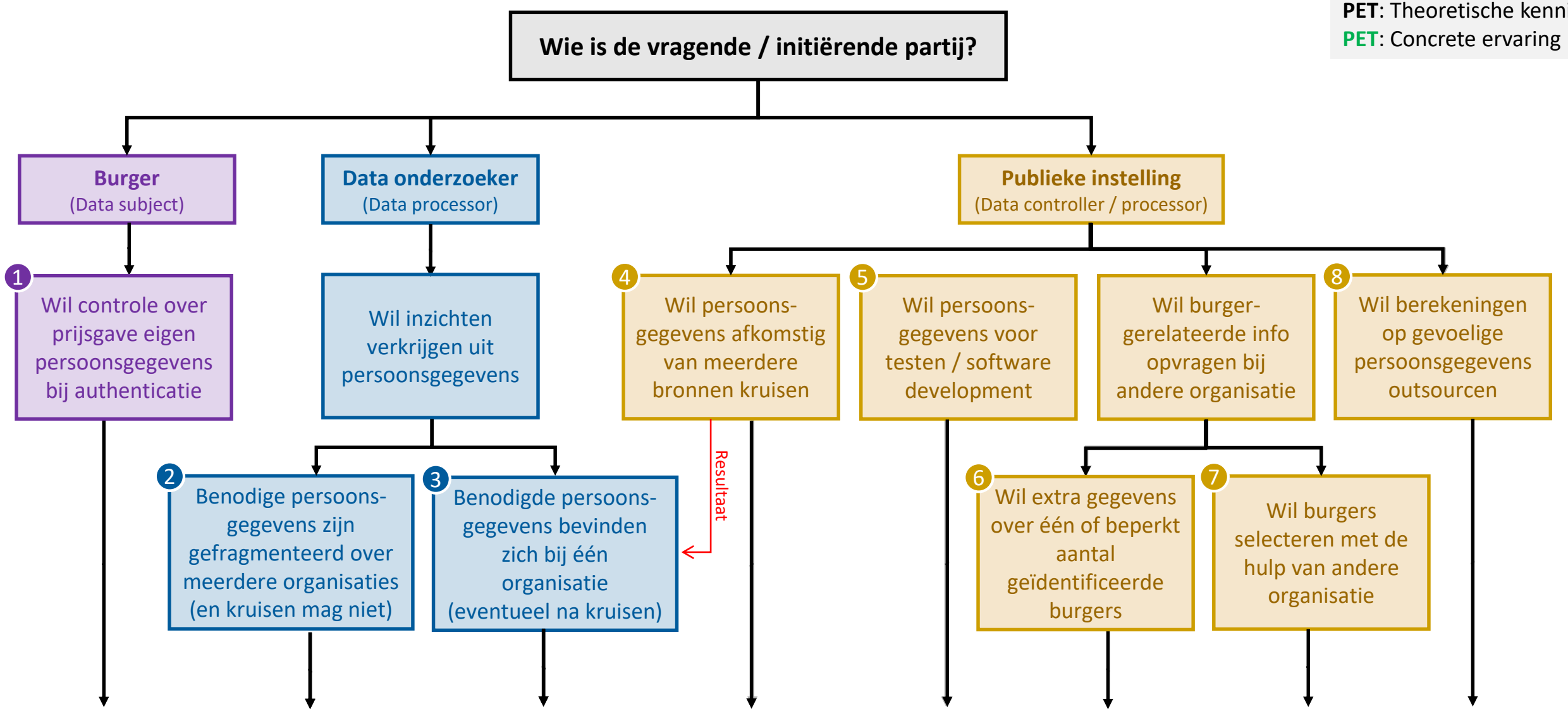
Trusted Execution Environtments (TEEs)

Homomorfe encryptie (HE)

Smals
ICT for society

Selectieboom

PET: Theoretische kennis
PET: Concrete ervaring



Afronding - Helicopterview

Onderzoek

KU LEUVEN

UCLouvain

Stanford University

Microsoft

IBM

En vele anderen

Heel veel ideeën, onderzoek & werk

Toepassingen & Commercialisering

- Cybernetica
- IBM
- Imec
- Microsoft
- NTT research
- Partisa
- Protegrity
- Roseman Labs
- TripleBlind
- Unbound
- …

Hier en daar (voorzichtig) toegepast
Interesse & investeringen ↗

Hype

Gartner

Beginnende hype

Goed moment om te kijken wat wij met PETs kunnen doen

Gartner. Top Strategic Technology Trends for 2022: Privacy-Enhancing Computation. 18 Oktober 2021
https://www.gartner.com/en/documents/4006926/top-strategic-technology-trends-for-2022-privacy-enhancing-computation

Smals ICT for society

Afronding – Let's start!

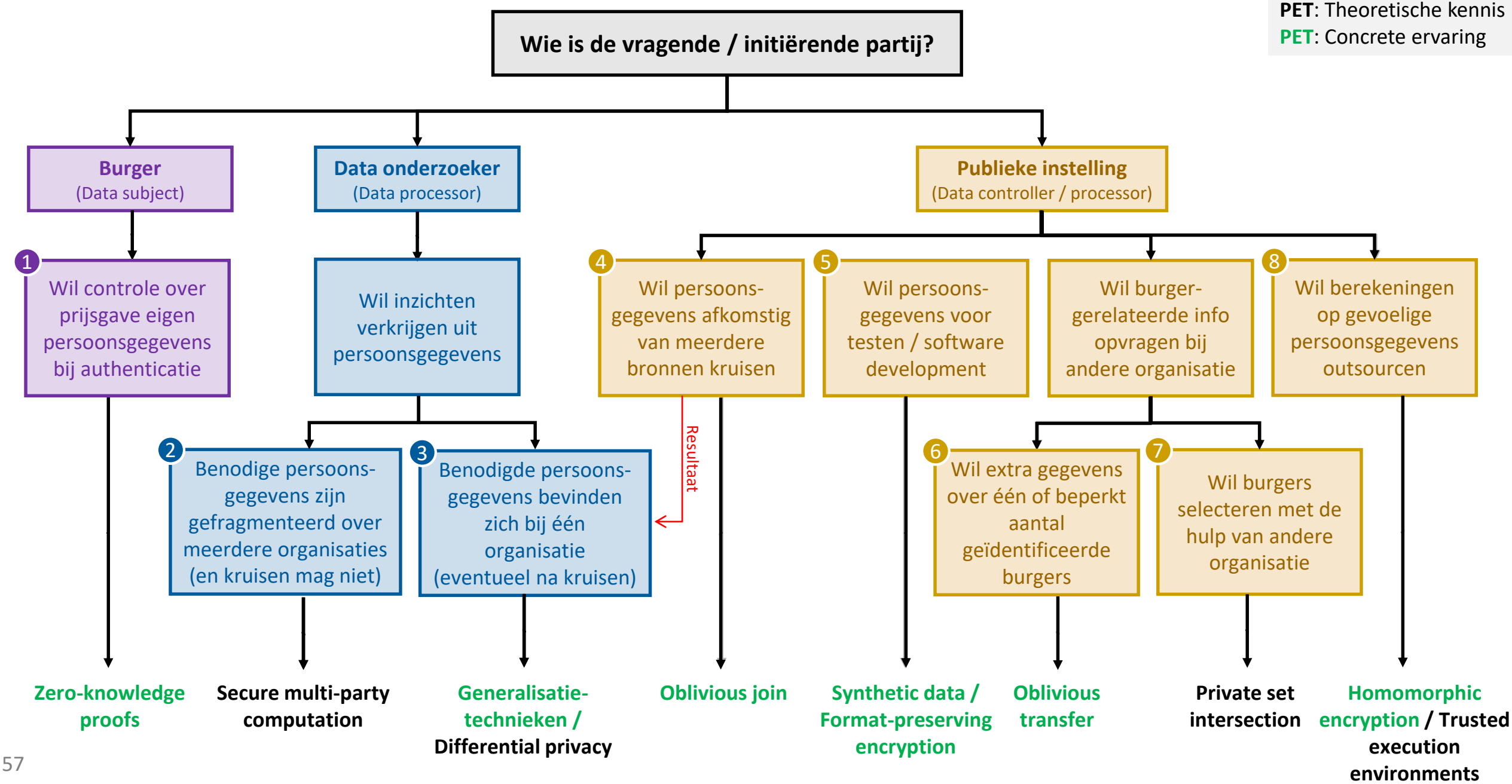
Er is meer dan wat in webinar aan bod kwam	Soms verrassende toepassingen	Publieke sector experimenteert (vb. Nederland, Estland)	Onze universiteiten = wereldautoriteit	Smals Research als brug met publieke sector

Ziet u nuttige toepassingsmogelijkheden? Laat het ons weten!

Smals
ICT for society

PEILING: Welke PETs hebben volgens u het meest potentieel en verdienen dus meer aandacht?

PET: Theoretische kennis
PET: Concrete ervaring



Contact / Blogposts / Vragen

Kristof Verslype

Cryptographer, PhD
Smals Research

Smals
ICT for society

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

"Vergeetachtige verzending" voor vertrouwelijk onderzoek naar personen

Posted on 18/06/2019 by Kristof Verslype

Geregeld is onderzoek nodig naar verdachte personen. Dit neemt niet weg dat de privacy van deze en andere personen gerespecteerd moet worden. Ook de confidentialiteit van het onderzoek moet gegarandeerd blijven. Dit artikel reikt een waardevolle technologie aan om aan … Continue reading →

Bescherming van persoonsgegevens met geavanceerde cryptografie

Posted on 17/09/2019 by Kristof Verslype

De bescherming van persoonsgegevens is cruciaal voor overheidsinstellingen. Toch blijkt het vaak moeilijk om een evenwicht te vinden tussen veiligheid, kost, functionele vereisten en gebruiksgemak. Daar waar traditionele benaderingen geen bevredigende oplossingen bieden, kunnen geavanceerde cryptografische tools mogelijks een

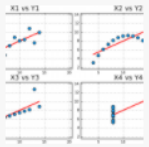
Differential Privacy

Posted on 12/01/2021 by Christophe Debruyne

Met GDPR, van toepassing sinds mei 2018, voorschrijft de EU de regels voor de verwerking van persoonsgegevens door bedrijven en overheden van EU burgers. Om persoonlijke gegevens in een dataset te beschermen gaat men al te vaak de persoonlijke gegevens … Continue reading →

Synthetic Data

Posted on 28/10/2020 by Joachim Ganseman



Als het moeilijk of duur is om aan echte gegevens te geraken, kan je soms al ver geraken met een goed substituut. In deze blogpost gaan we dieper in op de mogelijkheden van synthetische data. Continue reading →

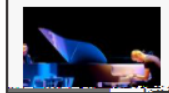
Privacybevorderende technologieën voor de publieke sector

Posted on 12/10/2021 by Kristof Verslype

Het wordt steeds makkelijker om grote hoeveelheden persoonsgegevens te verzamelen en te verwerken. Dit creëert enerzijds heel wat opportuniteiten, zoals het doen van statistische analyses ter verbetering van de gezondheidszorg. Tegelijkertijd moet echter rekening gehouden worden met de privacy van … Continue reading →

Secure multiparty computation – Collectieve berekeningen op verspreide gevoelige gegevens

Posted on 08/06/2021 by Kristof Verslype



Binnen de cryptografie bestaat een stelling die zegt dat alles wat met behulp van een centrale partij (Facebook, Amazon, de overheid, …) berekend kan worden in principe ook zonder die centrale partij berekend…

https://www.smalsresearch.be/blog/

Smals
ICT for society