COSIC

dp^{3}t

imec
embracing a better life

KU LEUVEN

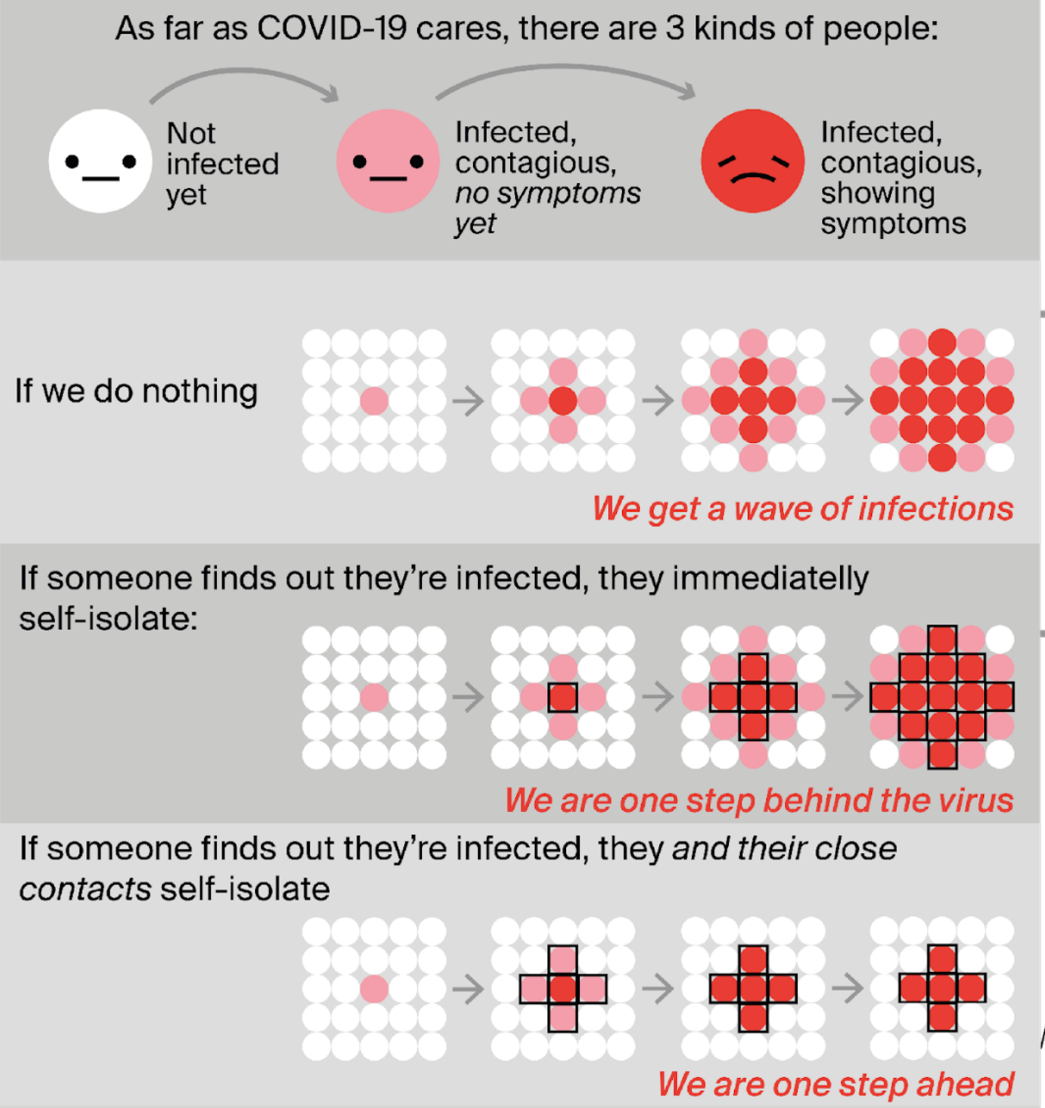
Privacy-Preserving Proximity Tracing

Bart Preneel

Bart.Preneel(AT)esat.kuleuven.be
@cosic.be

16June 2020

What is contact tracing ?



As far as COVID-19 cares, there are 3 kinds of people:

Not infected yet

Infected, contagious, *no symptoms yet*

Infected, contagious, showing symptoms

If we do nothing

We get a wave of infections

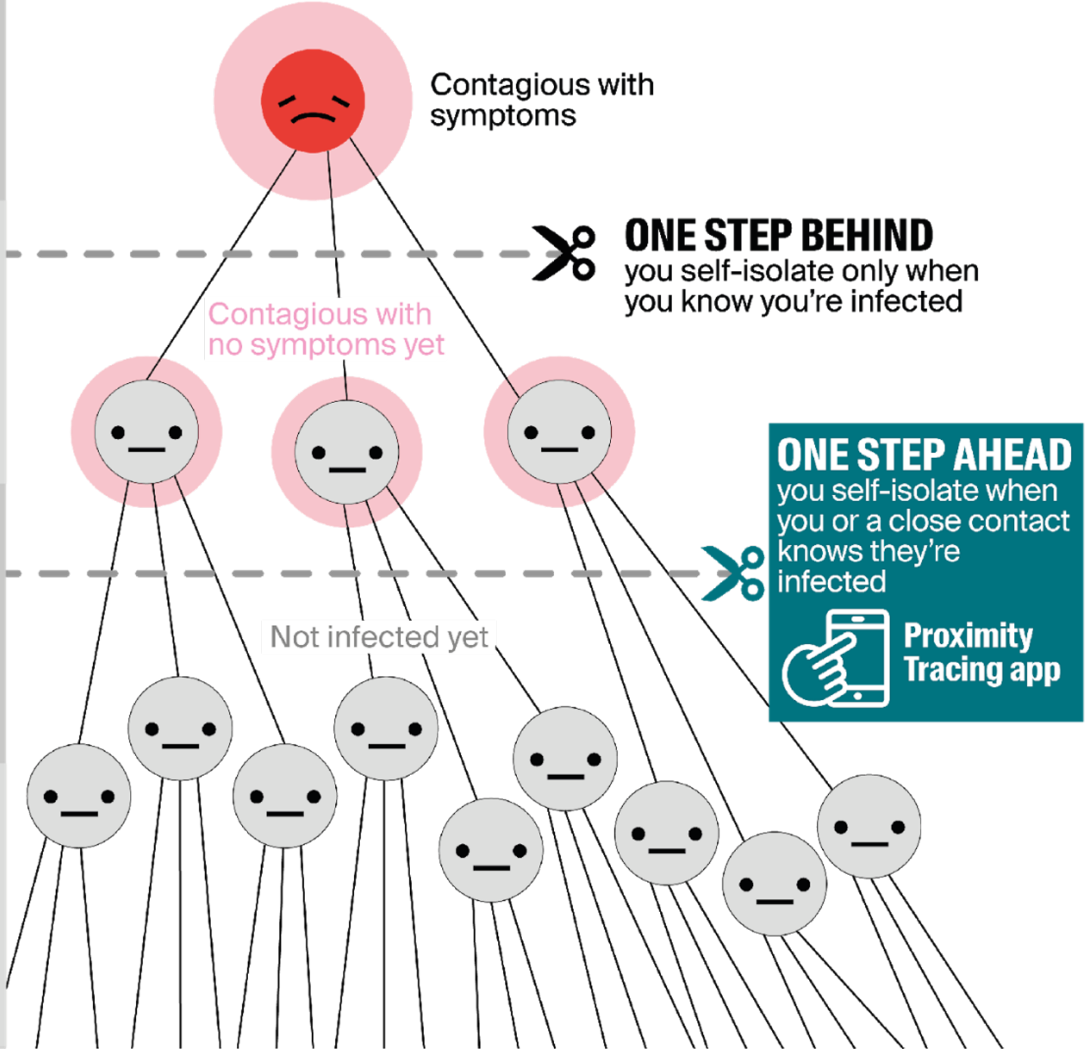
If someone finds out they're infected, they immediatelly self-isolate:

We are one step behind the virus

If someone finds out they're infected, they *and their close contacts* self-isolate

We are one step ahead

Test-Isolate-Quarantine



Contagious with symptoms

ONE STEP BEHIND
you self-isolate only when you know you're infected

Contagious with no symptoms yet

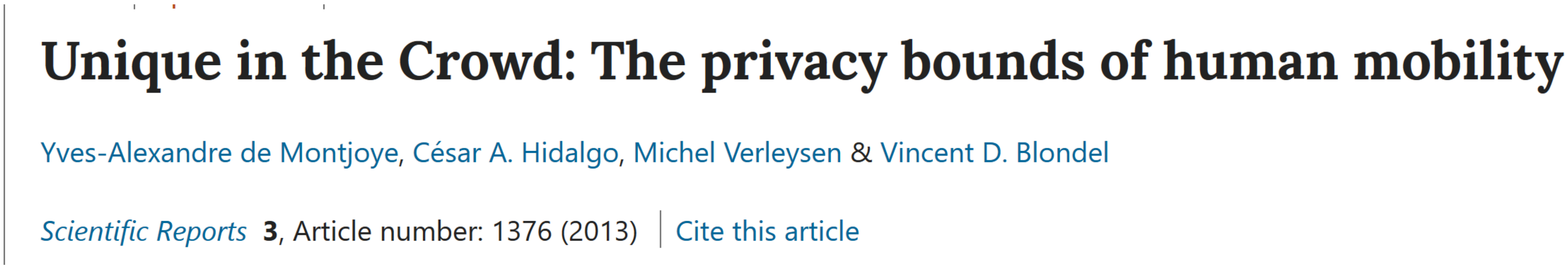
ONE STEP AHEAD
you self-isolate when you or a close contact knows they're infected

Proximity Tracing app

Not infected yet

Proximity tracing: geolocation (GPS)

- Examples: South-Korea, Israel (+ Google location data), Norway
- Major privacy problem: 4 space-time points identify 95% of individuals



Unique in the Crowd: The privacy bounds of human mobility

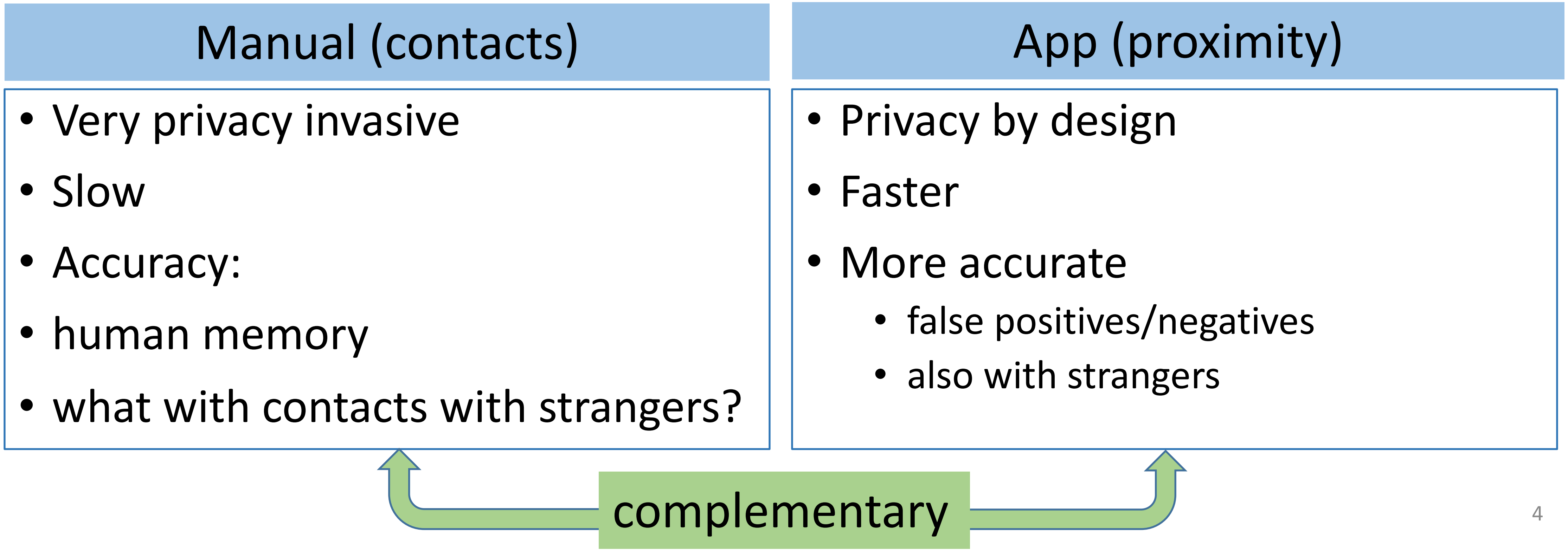
Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen & Vincent D. Blondel

Scientific Reports **3**, Article number: 1376 (2013) | Cite this article

The picture can't be displayed.

Contact tracing
= essential to control epidemic

Conditions:
- Not too many infections
- Sufficient testing
- Sufficient capacity



Manual (contacts)

- Very privacy invasive
- Slow
- Accuracy:
- human memory
- what with contacts with strangers?

App (proximity)

- Privacy by design
- Faster
- More accurate
    - false positives/negatives
    - also with strangers

complementary

Goal of contact tracing

- Warn citizens at risk
- Encourage citizens to undergo a test or to go in quarantine
- (contribute to epidemiological research) (opt-in)

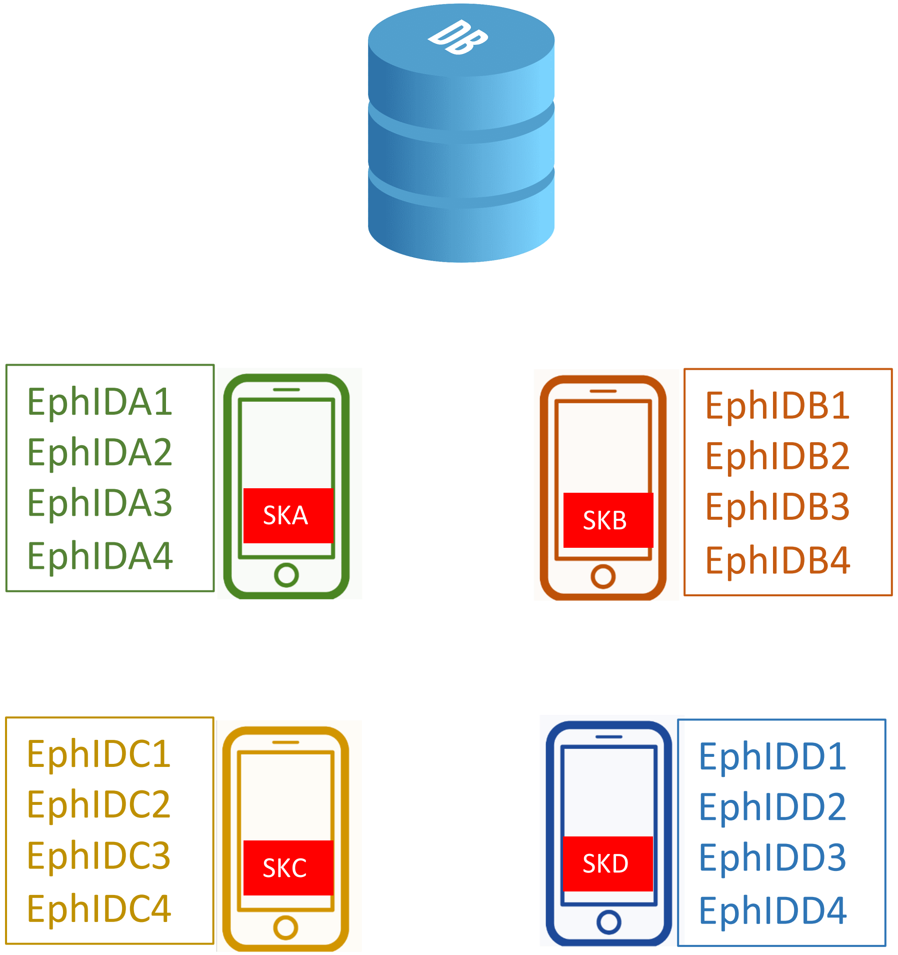
Respect for privacy and human rights

- Data minimization – privacy by design (GDPR)
  - No central database that can reconstruct social count
- Data can only be used to detect proximity
  - Built-in protection against "function creep"
- Protect identities: who has been in contact with whom, where and when
  - No information about uninfected users
- Right to be forgotten (erase data): auto-fading

Proximity tracing: other requirements

- Accuracy:
  - Only for sufficiently intensive contacts
  - Minimize false negatives and false positives
- Security: avoid false or incorrect reporting of infections (i.e. no self-reporting)
- Scalable to 10+ million users
- Deployable within 4-6 weeks
- Voluntary
- Transparency
- Interoperability

installation



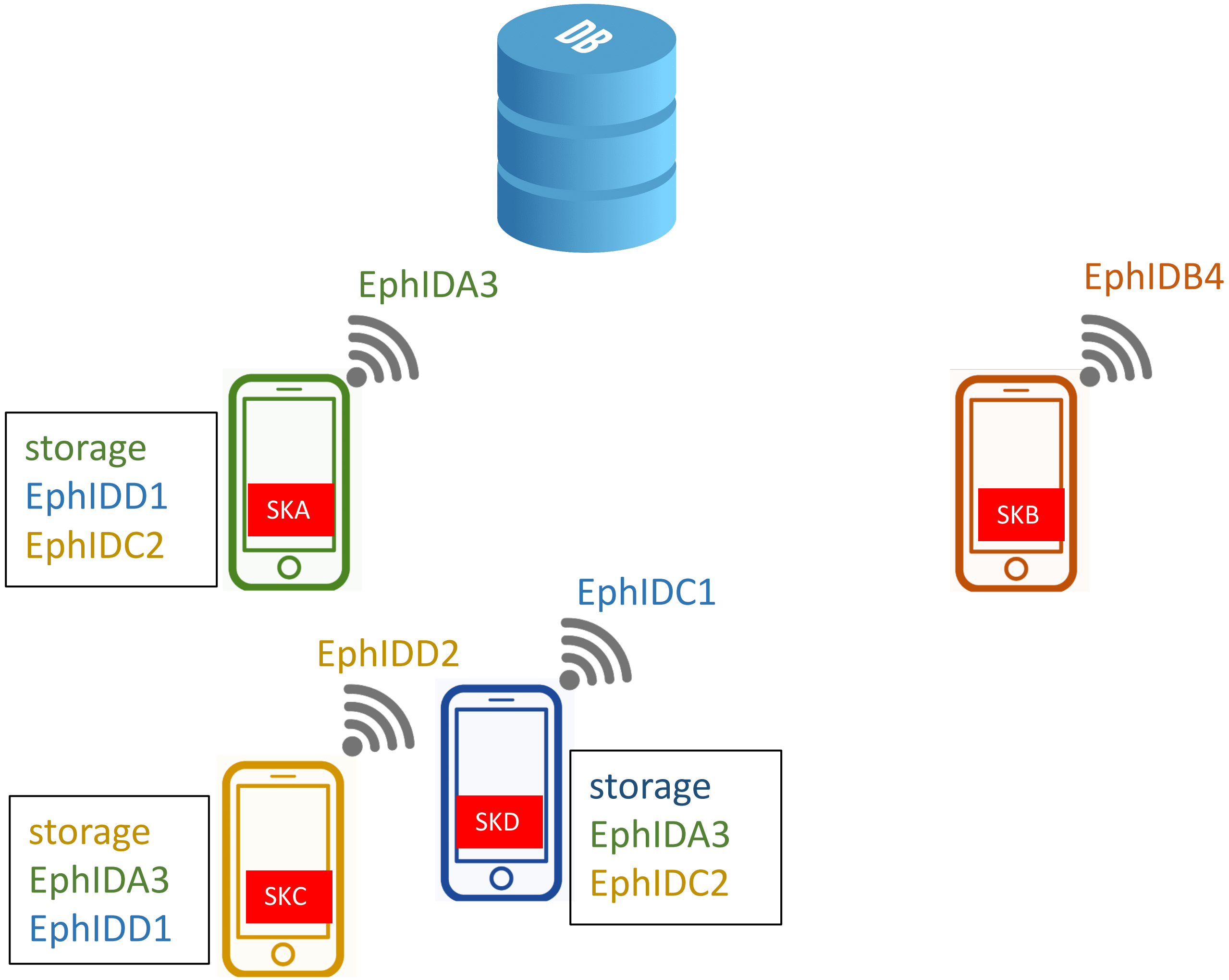
EphIDA1
EphIDA2
EphIDA3
EphIDA4

EphIDB1
EphIDB2
EphIDB3
EphIDB4

EphIDC1
EphIDC2
EphIDC3
EphIDC4

EphIDD1
EphIDD2
EphIDD3
EphIDD4

operation

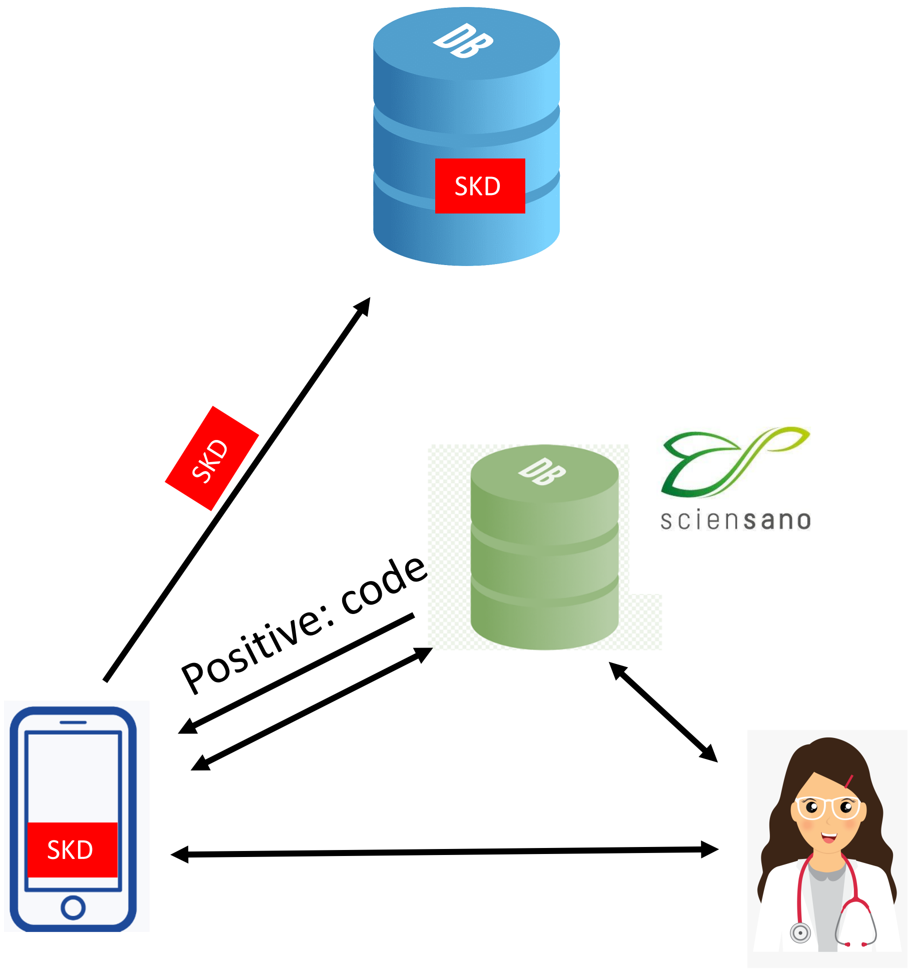


storage
EphIDD1
EphIDC2

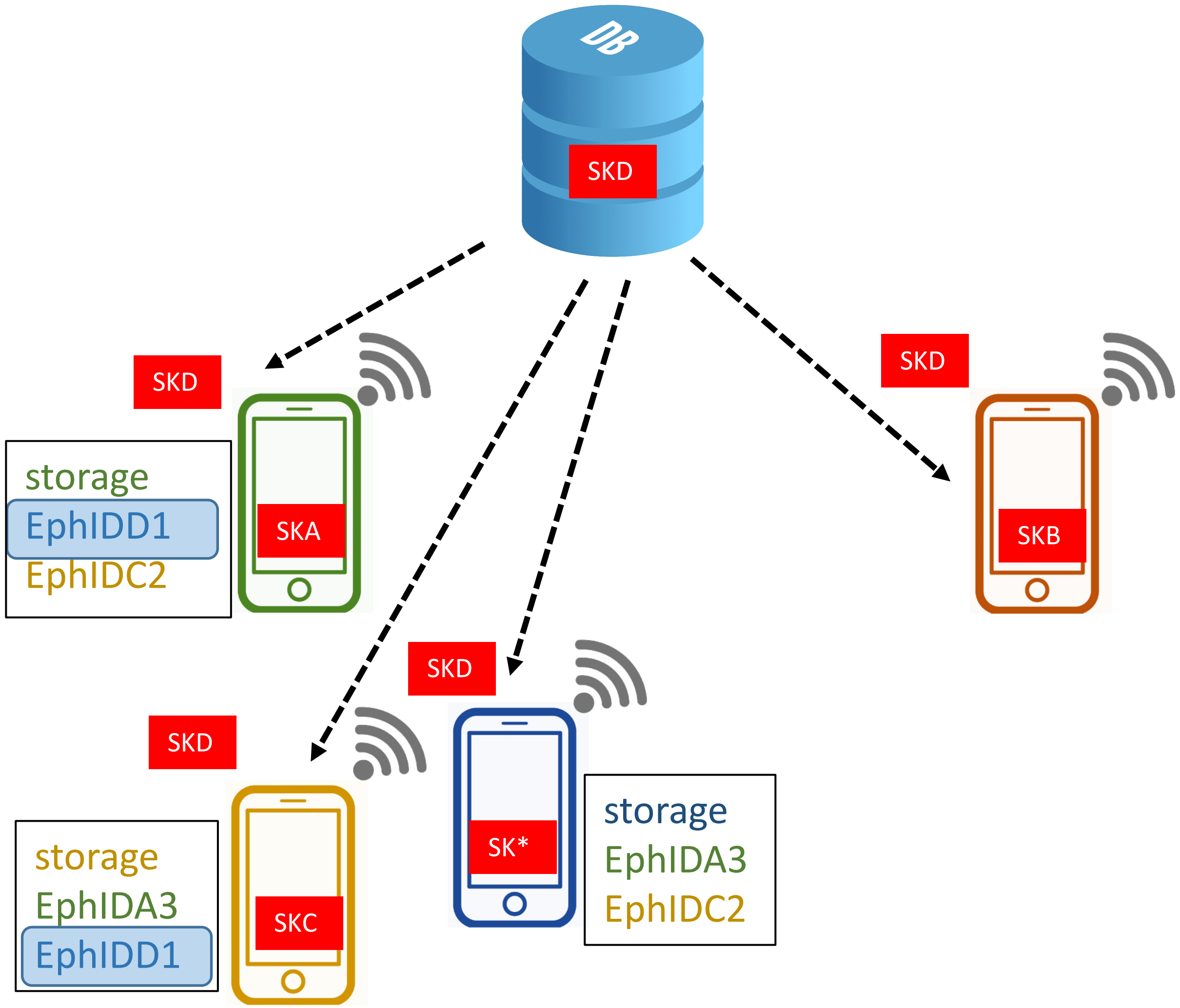
storage
EphIDA3
EphIDD1

storage
EphIDA3
EphIDC2

test



proximity tracing



Protocol 3b: polling variant

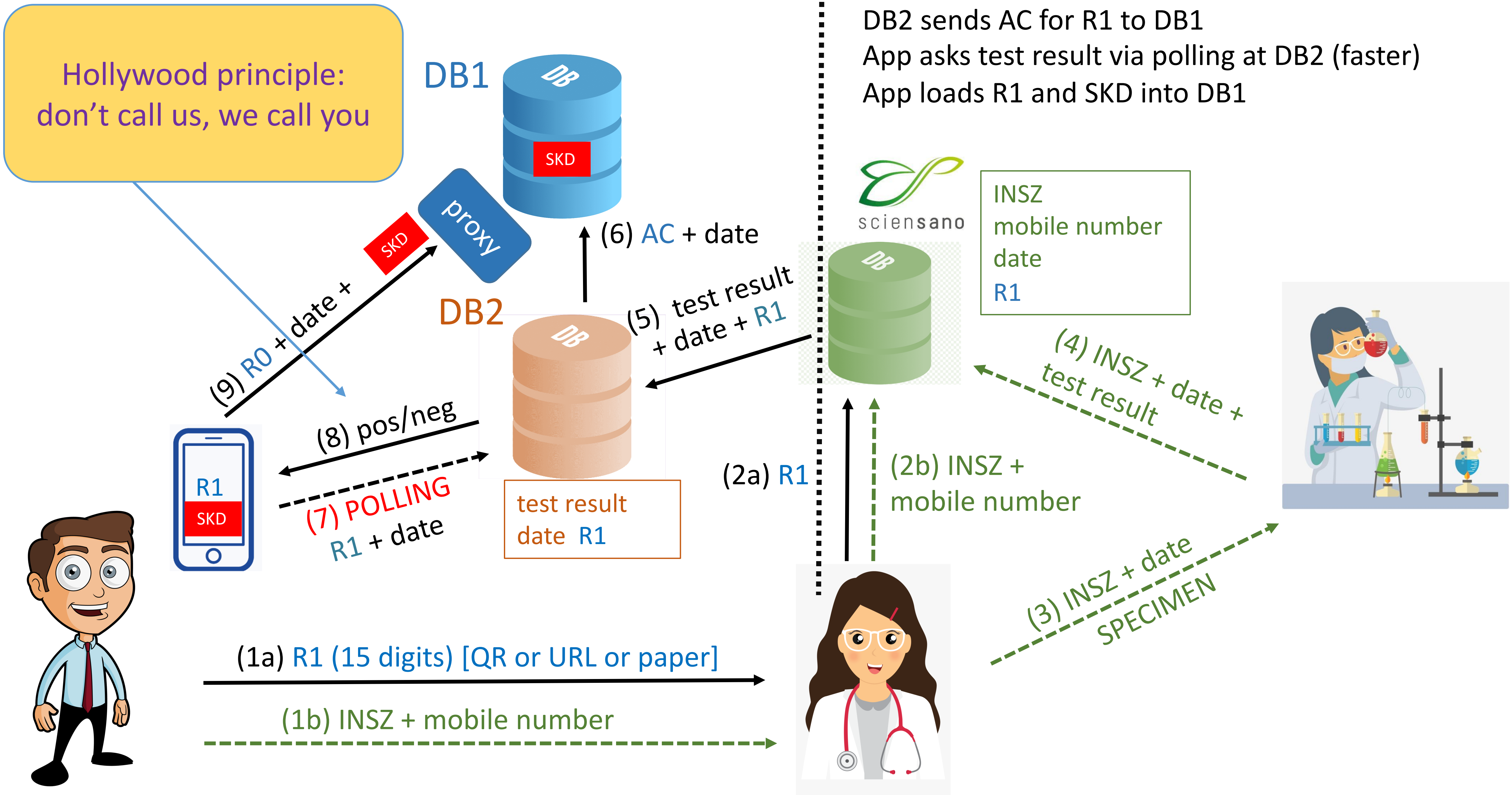
Test is linked to app via random code R1 = H(SKD,R0) (R0 = 128-bit random string)

Test result with R1 for short time in database DB2

DB2 sends AC for R1 to DB1

App asks test result via polling at DB2 (faster)

App loads R1 and SKD into DB1



Hollywood principle: don't call us, we call you

(1a) R1 (15 digits) [QR or URL or paper]

(1b) INSZ + mobile number

(2a) R1

(2b) INSZ + mobile number

INSZ
mobile number
date
R1

(3) INSZ + date SPECIMEN

(4) INSZ + date + test result

(5) test result + date + R1

test result
date R1

(6) AC + date

(7) POLLING R1 + date

(8) pos/neg

(9) R0 + date + SKD

DP-3T: https://github.com/DP-3T documents and code under de Mozilla Public License

EPFL: **Prof. Carmela Troncoso,** Prof. Mathias Payer, Prof. Jean-Pierre Hubaux, Prof. Marcel Salathé, Prof. James Larus, Prof. Edouard Bugnion, Dr. Wouter Lueks, Theresa Stadler, Dr. Apostolos Pyrgelis, Dr. Daniele Antonioli, Ludovic Barman, Sylvain Chatel

ETHZ: Prof. Kenneth Paterson, Prof. Srdjan Capkun, Prof. David Basin, Dr. Jan Beutel, Dennis Jackson

KU Leuven: Prof. Bart Preneel, Prof. Nigel Smart, Dr. Dave Singelée

TU Delft: Prof. Seda Gürses

University College London: Dr. Michael Veale

University of Oxford: Dr. Reuben Binns

CISPA: Prof. Cas Cremers, Prof. Michael Backes, Dr. Nils Ole Tippenhauer

University of Torino / ISI Foundation: Prof. Ciro Cattuto

Aix Marseille Univ, Université de Toulon, CNRS, CPT: Dr. Alain Barrat

University of Salerno : Giuseppe Persiano

IMDEA Software: Dario Fiore

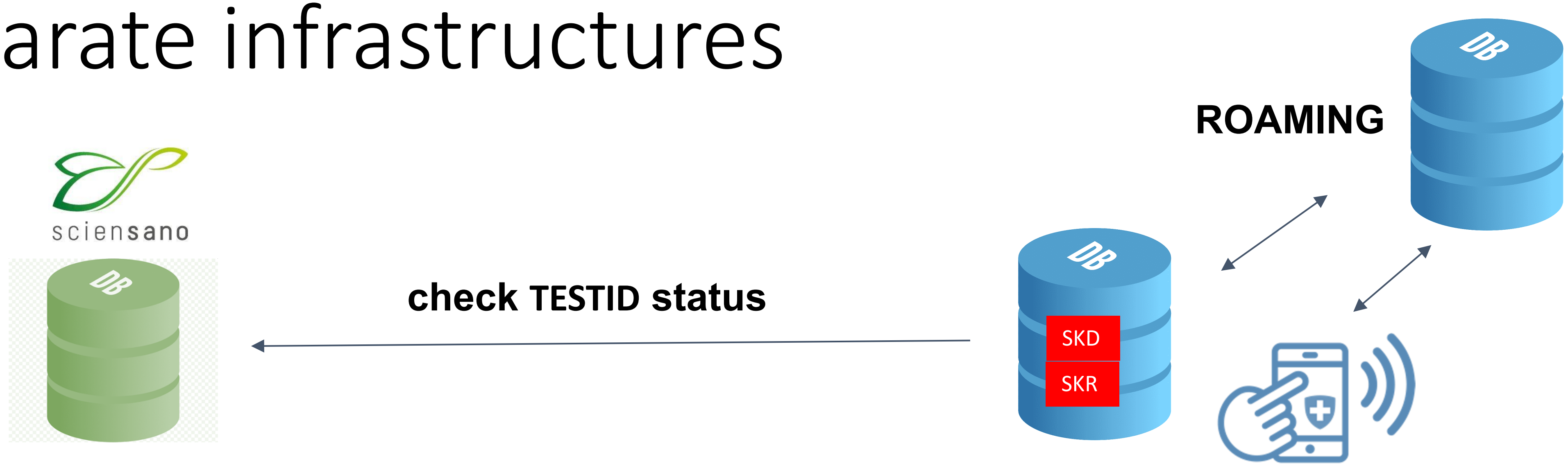
University of Porto (FCUP) and INESC TEC: Prof. Manuel Barbosa

Stanford: Dan Boneh

Bart Preneel, COSIC, at KU Leuven and imec

ADDRESS:	Kasteelpark Arenberg 10, 3000 Leuven
WEBSITE:	homes.esat.kuleuven.be/~preneel/
EMAIL:	Bart.Preneel@esat.kuleuven.be
TWITTER:	@CosicBe
TELEPHONE:	+32 16 321148

Separate infrastructures



Health System IT infrastructure

Case management

Medically-regulated environment

OUTSIDE SCOPE OF DP-3T

DP-3T Infrastructure

Anonymous

Not medically regulated

International exchanges for roaming purposes

Additional questions

- Role of Google and Apple
- Effectiveness
  - Critical Mass of Users
  - Accuracy
- Interoperability: which other countries choose the DP-3T approach?
- Is this a perfect system?

The Google/Apple Exposure API

- Apple: Bluetooth can't be used in background: app must run in the foreground and the phone should not be locked
- Google/Apple: access to Bluetooth radio details
- Solution: special interface, only for decentralized apps
  - DP-3T is in close consultation with development team
- No data to Google/Apple
- Interface is deactivated after pandemic

Effectiveness

- No scientific consensus on minimum share (could even be effective from 15-20% - e.g. 80% student participation only)
- Accuracy (false positives and negatives):
  - non-trivial problem but realistic expectation that it will suffice
  - user can erase certain periods

Interoperability

- DP-3T and/or Google/Apple architecture: Switzerland, Austria, Estonia, Finland, Latvia, Germany, Denmark, Italy, Ireland, Spain, the Netherlands, (Belgium)…
- Exchange of minimal information (keys) between countries: no sensitive information such as location or names
- Can be done by telephones or through national databases (cf. DP-3T interoperability document)

Is DP-3T perfect?

- Design offers strong privacy guarantees with maximum protection against misuse of central database (at the cost of increased risk of local attacks)
- But every system (manual or digital) for contact or proximity tracing leaks information