Interoperability between European digital contact tracing applications

Prof. Jorge García Vidal

Universitat Politècnica de Catalunya (UPC)
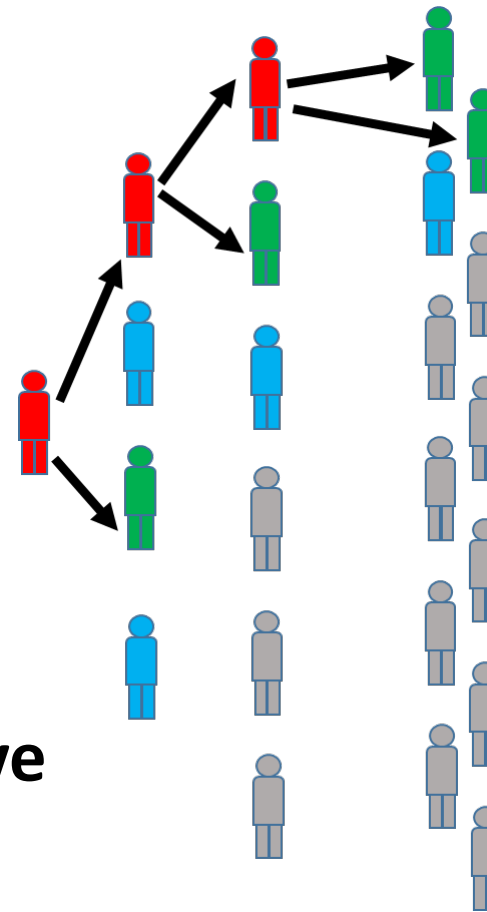
https://personals.ac.upc.edu/jorge/, jorge@ac.upc.edu

The promise of digital contact tracing

Exponential growth
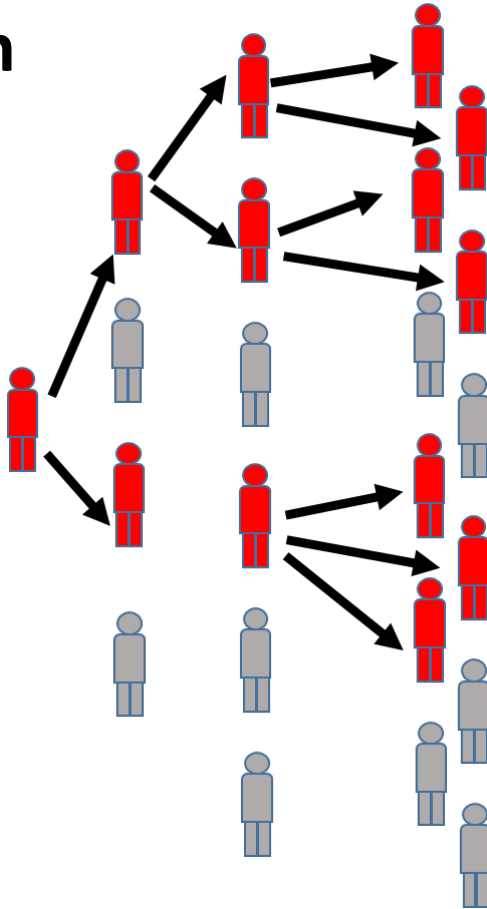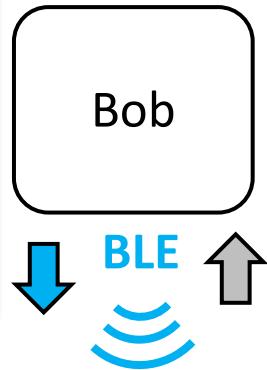
Cut transmission chains

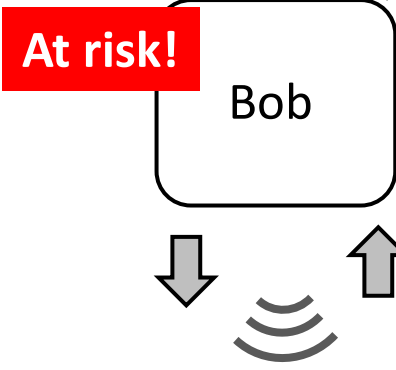**Risk exposure notification (e.g. self quarantine, isolate, test, etc)**

False positive

App operation

(1) Detect user in proximity
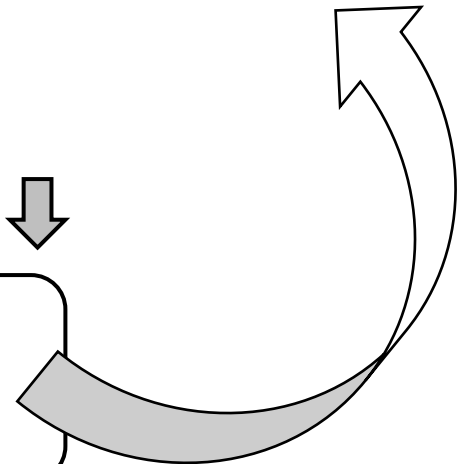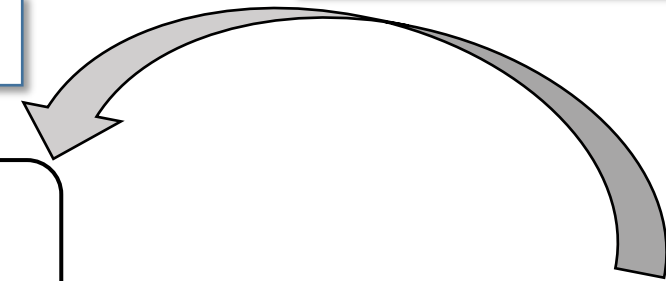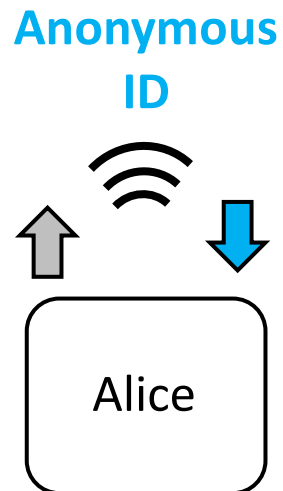(2) Exchange info through Bluetooth Low Energy (BLE).
(3) Estimate distance (RSSI)

Bob

BLE

Anonymous ID

Alice

(6) User is notified

At risk! Bob

(5) Exposure notification

Backend server

(4) Report of of COVID+ test

COVID+ Alice

BLE operation

Payload of beacons for ROBERT

ECC	EBID	Time	MAC
8 b	64 b	16 b	40 b

Payload of beacons for DP3T/GAEN

EphID
128 b

Broadcast model
- Use advertising mechanism of BLE
- Devices broadcast advertising packets
- Devices collect advertising packets, parses & stores the exchanged data
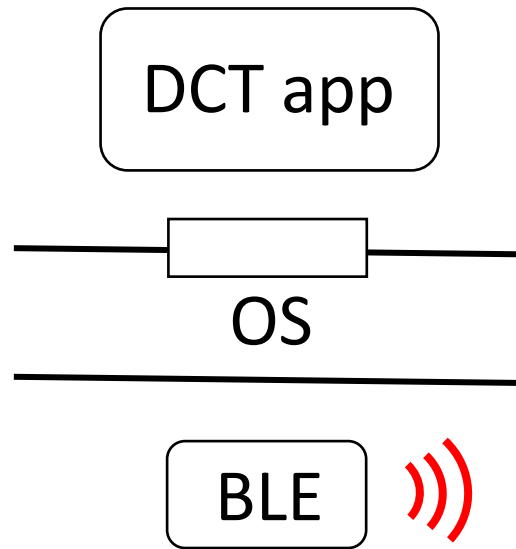- Only 20 Bytes may be used for data

Connected mode
- Devices advertises support to DCT
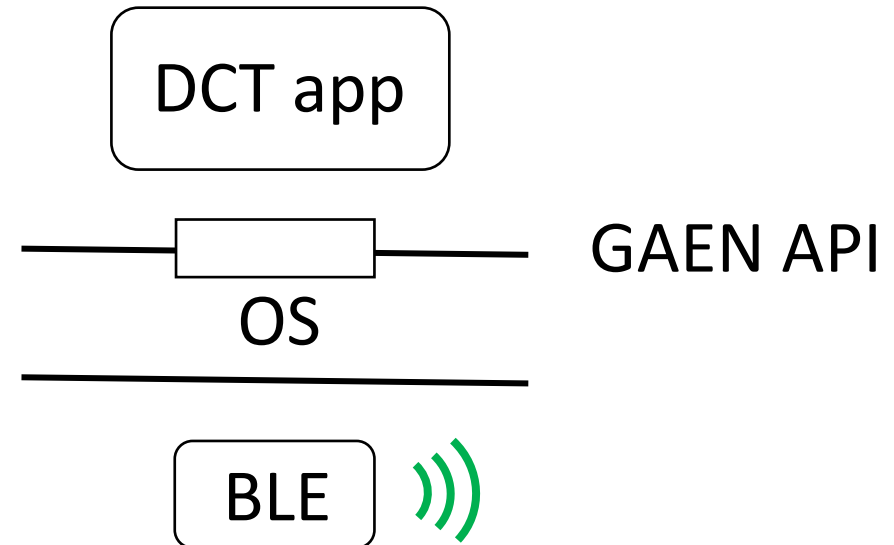- Establish a connection & exchange data

Hybrid mode
- Overcome limitations imposed by iOS
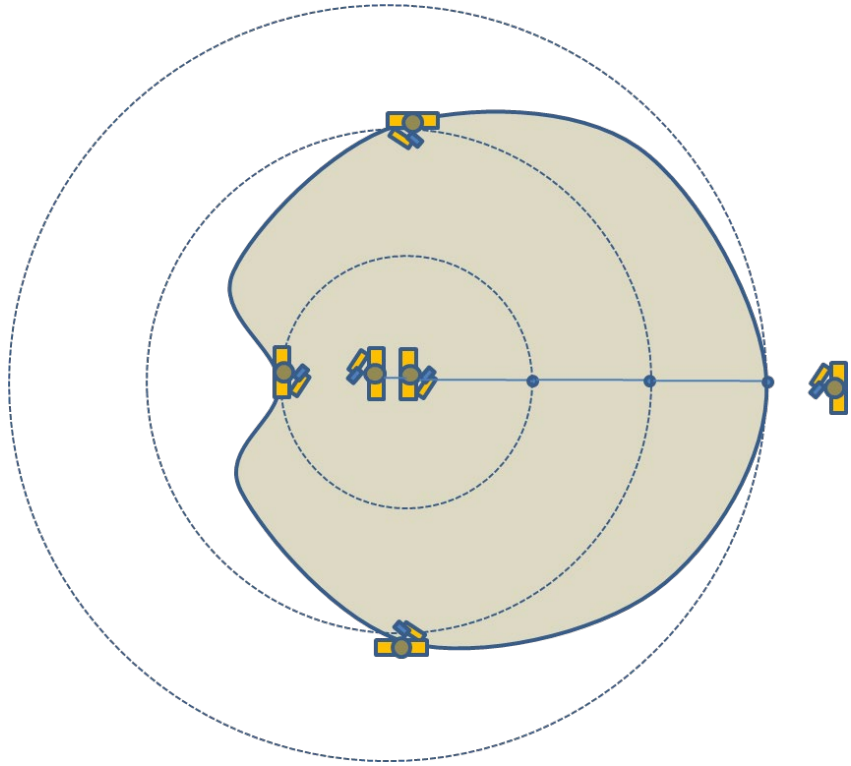
BLE operation & API

Anonymous IDs
processed by app

Anonymous IDs
processed by OS

DCT app

DCT app

OS

OS   GAEN API

BLE   BLE

Protocol imposed by the API (DP3T/GAEN)
Compatibility at BLE layer, Android/iOS
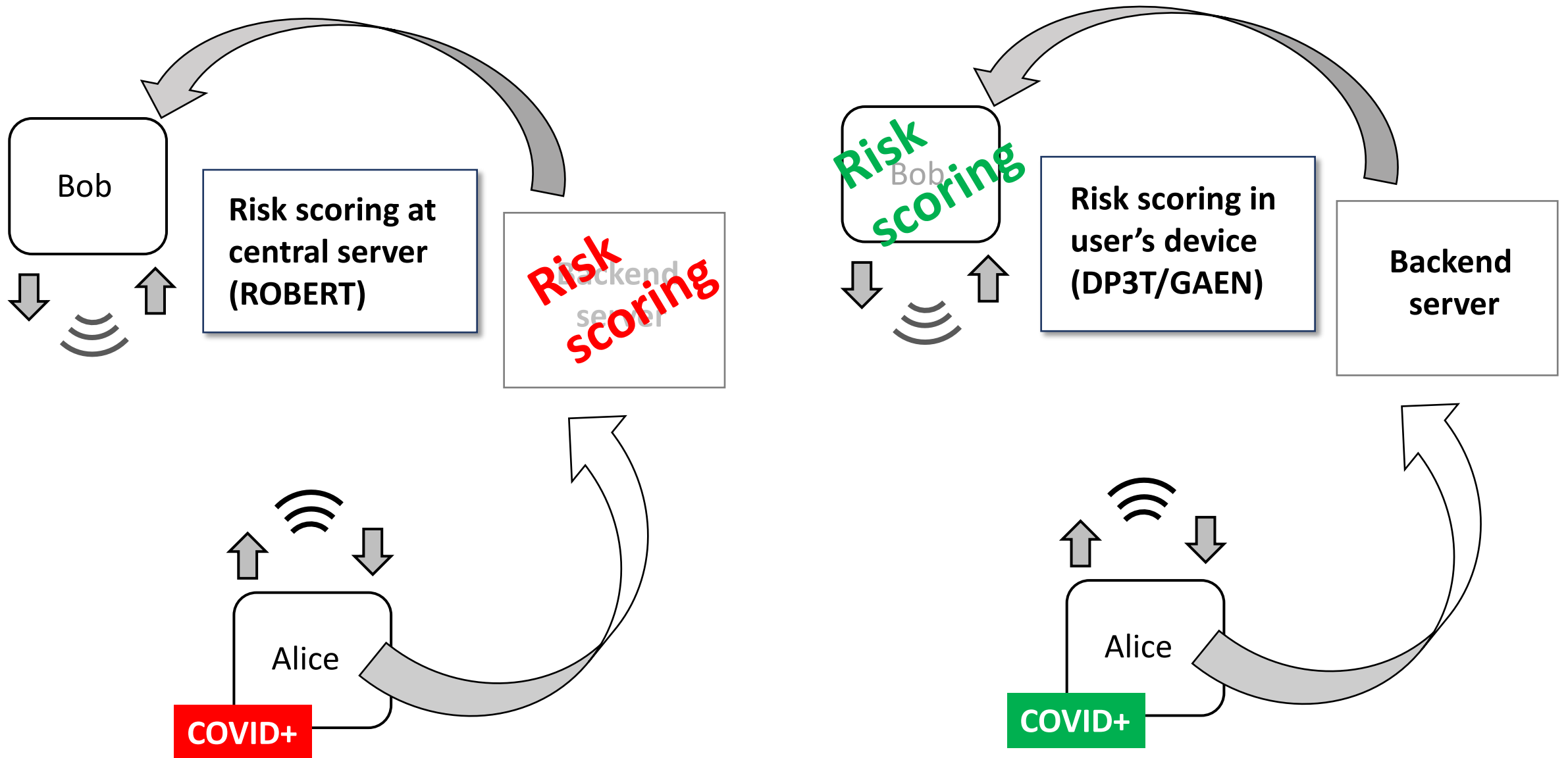
Using RSSI to estimate distance

BLE RSSI varies substantially depending on:
- the relative orientation of handsets,
- on absorption by the human body,
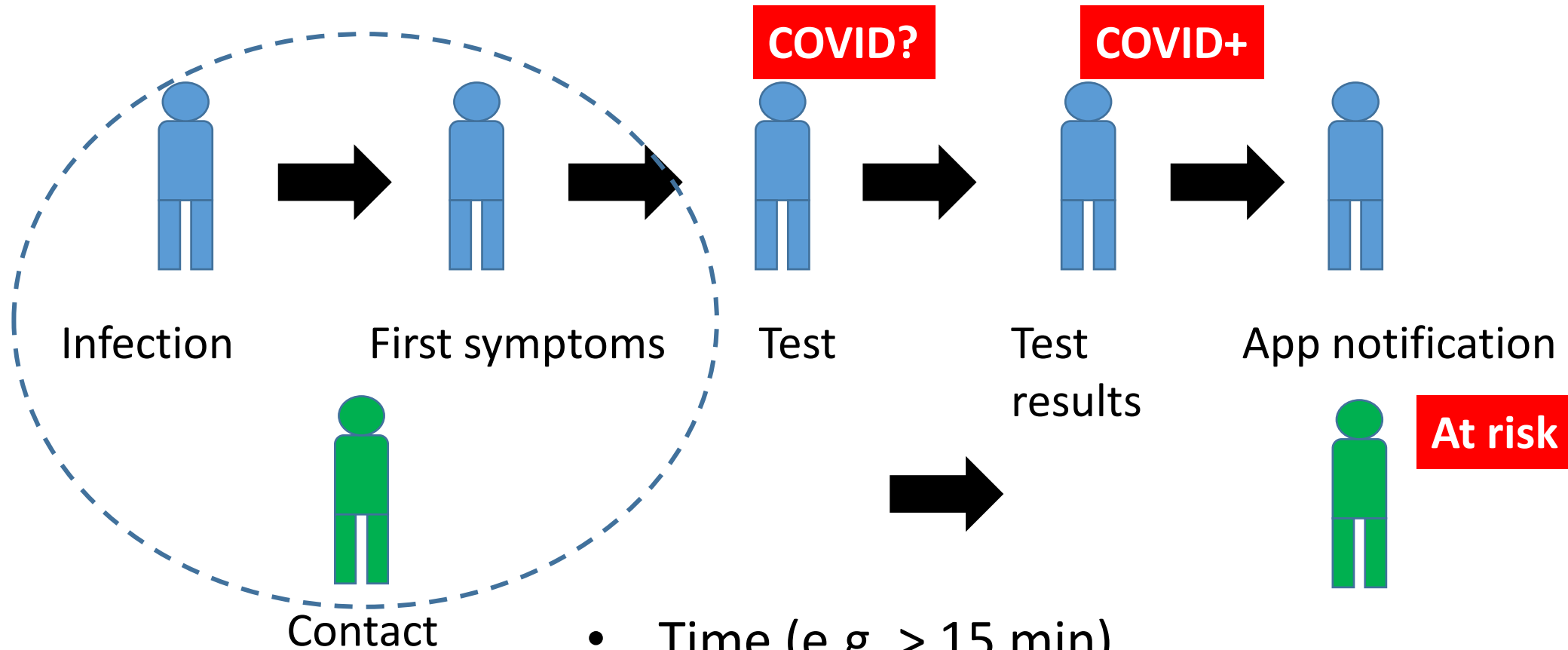- reflection/absorption of radio signals in buildings and trains.

Alternatives? :
- UWB, based on time of flight

Centralized vs decentralized

Integration with Health system & risk scoring

- Time (e.g. > 15 min)
- Distance (e.g. < 2 m)
- Other factors?: indoor/outdoor, mandatory mask, ventilation, etc

Interoperability

Upload all received diagnostic keys
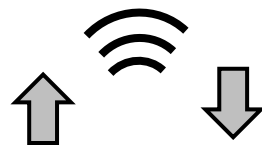
European Federated Gateway Service
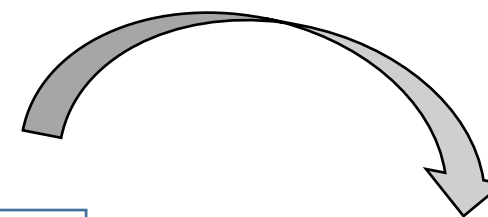
Backend server Country B

Backend server Country A

Risk scoring

Bob

Downloads all diagnostic keys from all other countries.

Alice

COVID+

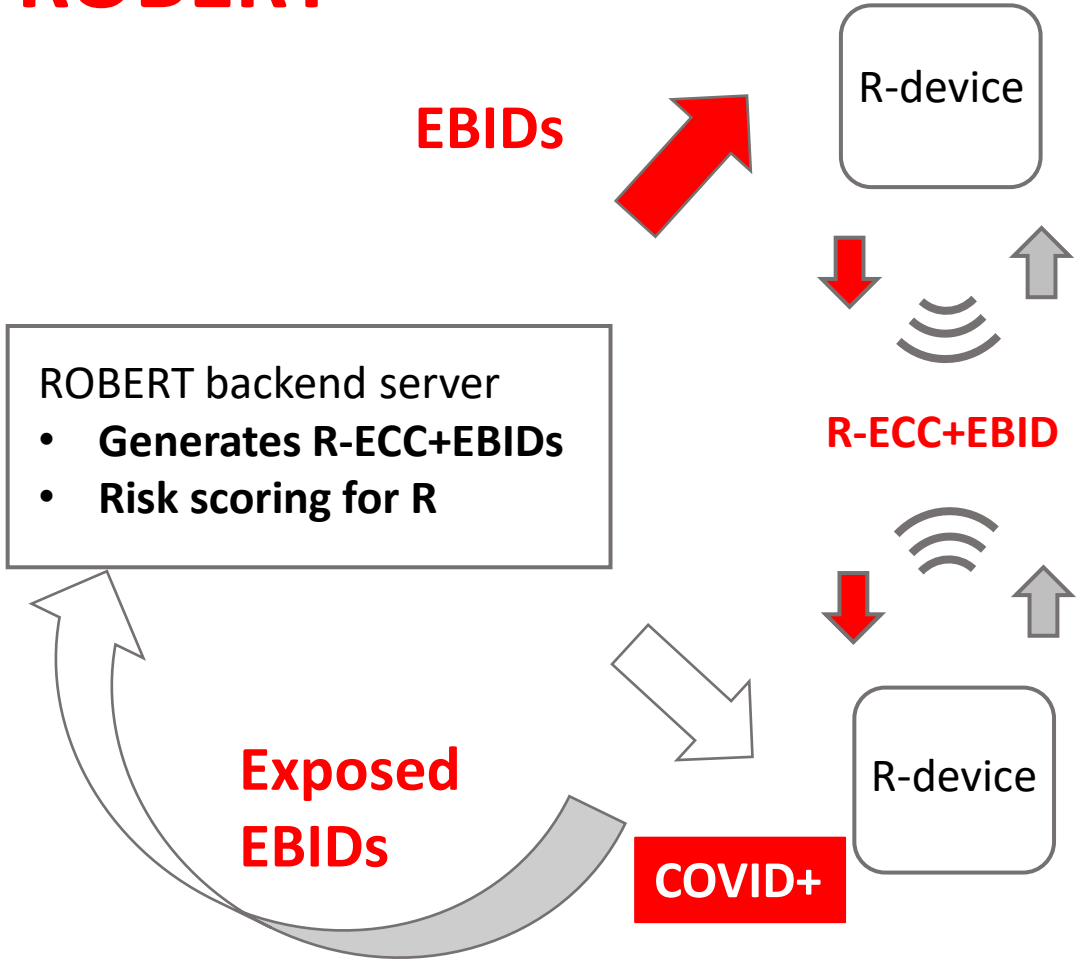Exposed keys & countries of interest (GAEN format)

Many complex issues ..

- Politically loaded issue, communication campaign
- Legal/Ethical issues (voluntary app)
- Integration with (public) health system (what should a user do when receives a "Risk exposure" notification?)
- Risk scoring (not well understood yet)
- Using BLE for distance estimation
- Population with no smartphones
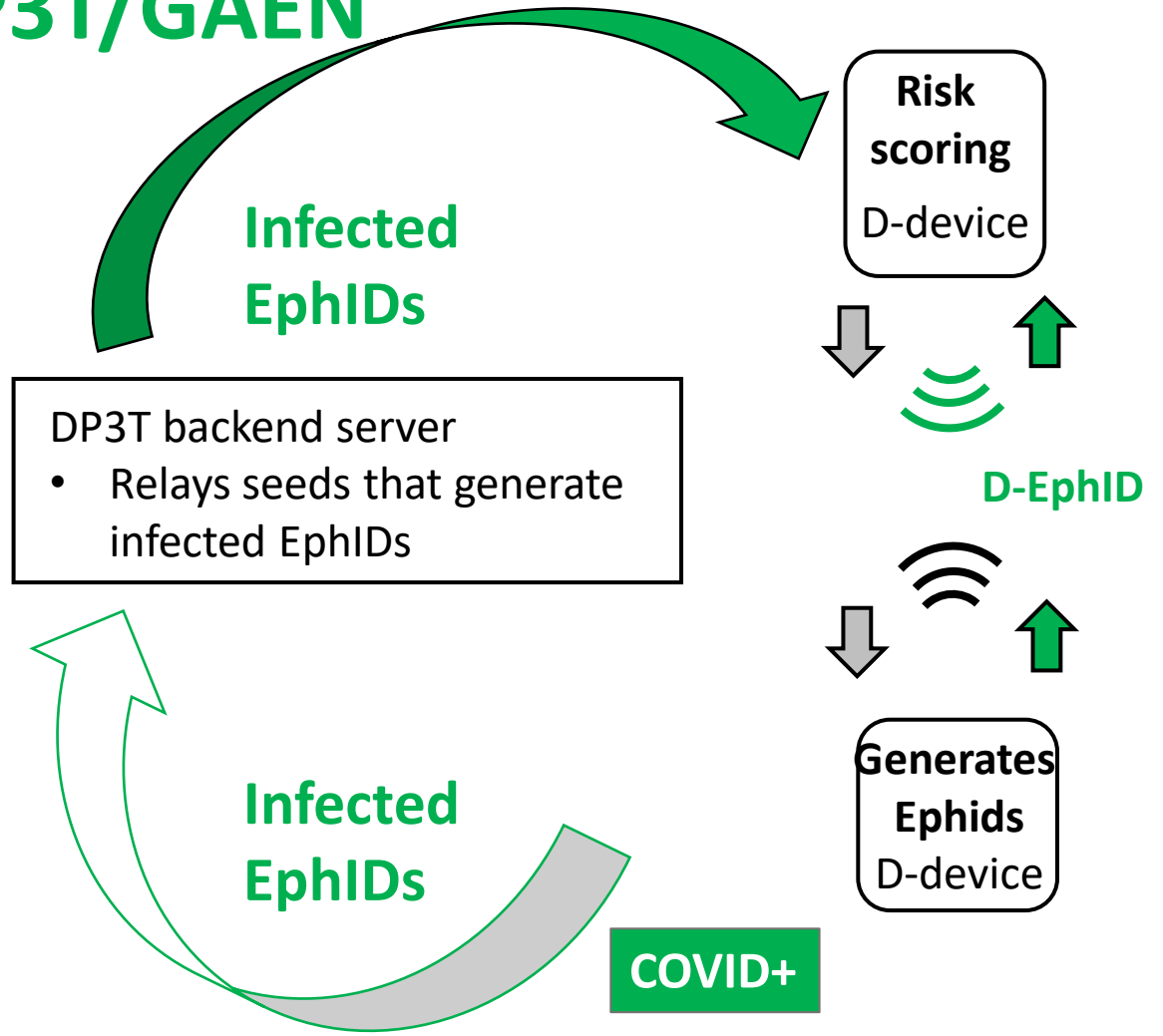- The role of Google & Apple
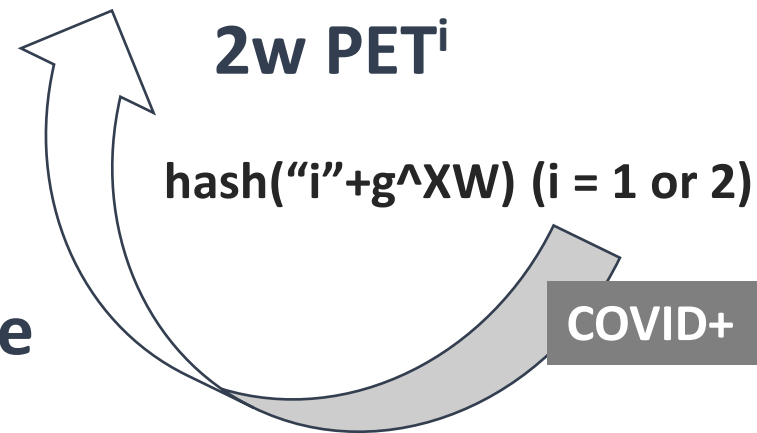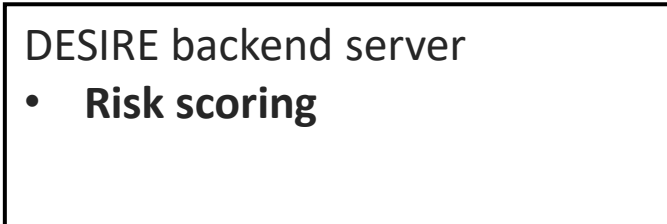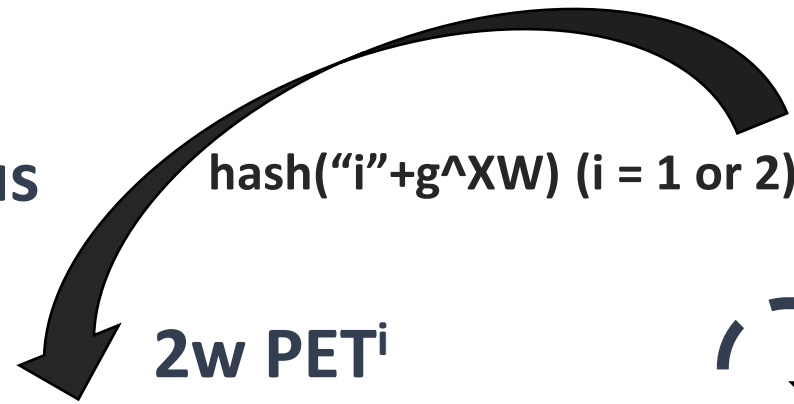- Interoperability

Thank you

DP3T/GAEN vs ROBERT

3rd way: DESIRE

Exposure Status Request

hash("i"+g^XW) (i = 1 or 2)

DES-device

Secret X

2w PET^i

DESIRE backend server
- **Risk scoring**

DES-EBIDs = g^X
DES-EBIDs = g^W

2w PET^i

hash("i"+g^XW) (i = 1 or 2)

COVID+

Secret W

DES-device

Infected Node Declaration