



# Contact Tracing mobile apps cross-border interoperability

eHealth Network

*Technical Experts – “Exposed keys” work stream*

2020-05-19

# Meeting purpose

Reach an agreement about the  
cross-border interoperability architecture

# Aspects to agree upon

## A. Keys specification

1. “BLE payload” → Proximity identifier exchanged between devices
2. “Exposed keys” → Temporary keys uploaded to the backend

## B. Backend architecture (*options*)

1. Backend federation
2. Backend federation + Forwarding gateway
3. Trusted Roaming

# Keys specification

Cross-border interoperability



# Keys specification

## “BLE payload”

- **What it is:** Proximity identifiers exchanged between devices
- *Any rotation mechanisms in place (e.g. “15 min” keys)?*

## “Exposed keys”

- **What it is:** Keys uploaded to the backend
- *What is the relevant information for risk calculation?*
- *Exchange of:*
  - *contact keys: keys of contacts detected in proximity*
  - *exposed keys: keys of contacts detected in high risk exposure*

# Backend architecture

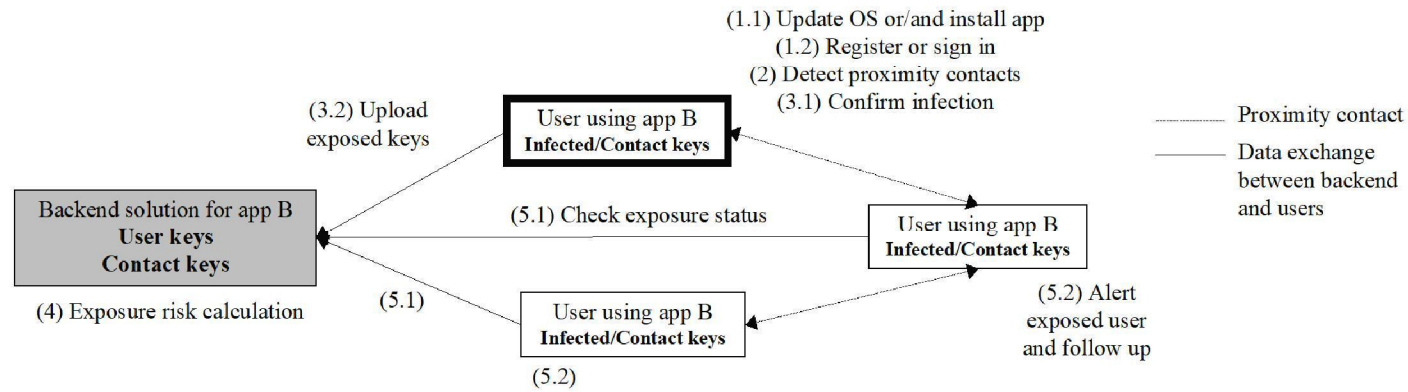
Cross-border interoperability



## Steps in the contact tracing flow

Number	Step	Description	Centralised
1	<b>Enable user with necessary technology</b>	When a user updates the mobile device operative system or/and installs a contact tracing app	(1.1) Update OS or/and install app (1.2) Register or sign in
2	<b>Proximity contact detection</b>	When activated by the user, the mobile device technology detects proximity contacts with other app users and record encounter details	(2) Detect proximity contacts
3	<b>Infection confirmation</b>	When an individual is informed, by the relevant authorities, about his/her positive test result for SARS-CoV-2	(3.1) Confirm infection (3.2) Upload contacts keys
4	<b>Exposure risk calculation</b>	When a proximity encounter exposure risk score is calculated	(4) Exposure risk calculation
5	<b>Exposure alert and follow up</b>	When a user gets an alert about possible exposure and possible follow up actions	(5.1) Check exposure status (5.2) Alert exposed user and follow up

# Steps in the contact tracing flow



## Backend architecture (possible options)

- How to identify the keys that should be exchanged?
  - Will there be a country code added to proximity identifier, or something else?
  - Do apps listen to the backend of their Member State only?

# Backend architecture (possible options)

## A. Backend federation

- What it is:

- ...

## B. Backend federation + forwarding gateway

- What it is:

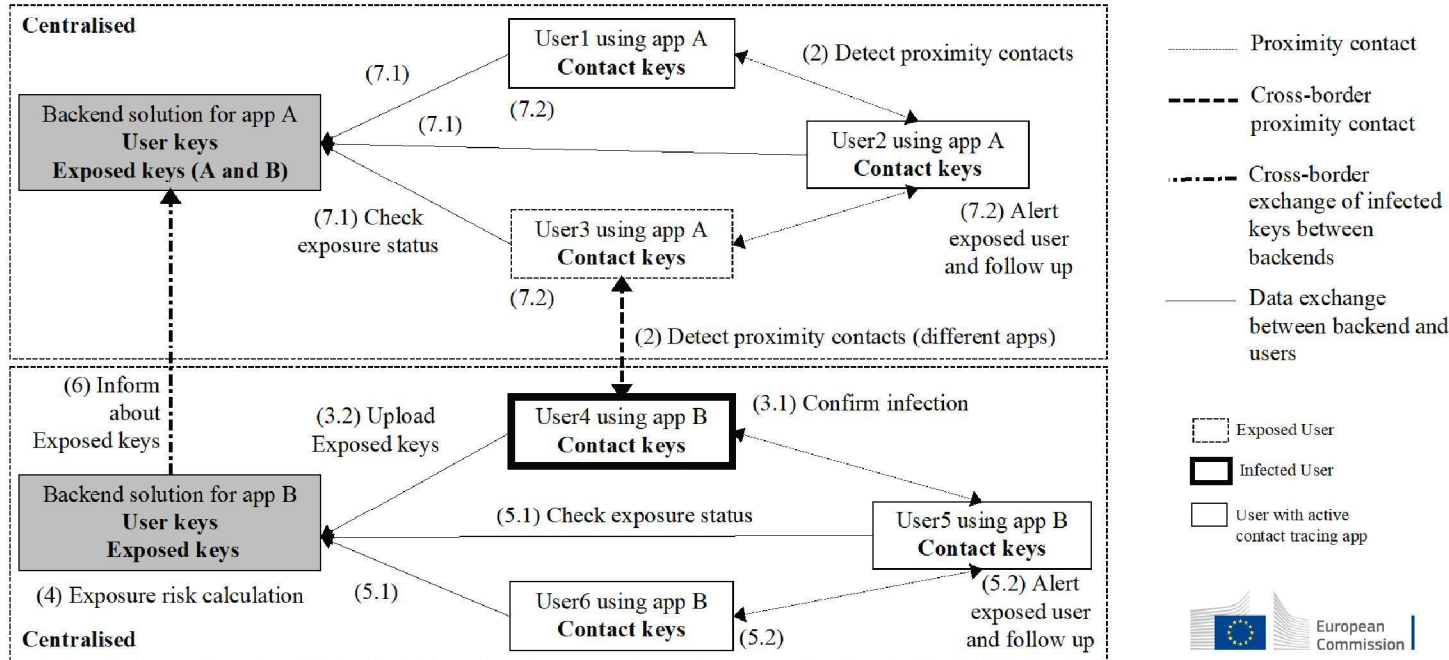
- ...

## C. Trusted Roaming

- What it is:

- ...

# Decentralised to decentralised



# Legal aspects

Cross-border interoperability



## Aspects to agree upon

A. What kind of data are being exchanged?

1. *Anonymous*
2. *Pseudonymous*

B. *Agreement between MS for interoperability of backend servers?*

C. *Use of Decision 1082/2013/EU?*