Contact Tracing mobile apps cross-border interoperability

eHealth Network

Technical Experts – "Exposed keys" work stream

2020-05-25

Meeting purpose

Agree on cross-border interoperability arrangements:

1. Keys specification [*country code encryption*]
2. Backend – federated architecture

Keys specification

Cross-border interoperability

Keys specification

"BLE payload"

- **What it is**: Proximity identifiers exchanged between devices

⇒*The constraint may be smoothed/interoperability easy to achieve*

⇒ *Standardization issue about the payload, to be checked with ETSI (E4P, Europe for Privacy Preserving Pandemic Protection)*

"Exposed keys"

- **What it is**: Keys uploaded to the backend
- *What is the relevant information for risk calculation?*
- *Upload of:*
  - *exposed keys: keys of contacts detected in high risk exposure*
  - *could be filtered on the device*

Keys specification

- "BLE payload" – Keys Specification
- FR and NO agreed on apps uploading "*Exposed Contacts keys*" to servers
- FR informed to have a *country code* (encrypted) in the payload. NO confirmed not having a country code but could add it.
- FR informed that *country code encryption, follows a FR strict encryption formula*. ***Can it be shared or commonly agreed with NO?***
- **Can FR app collect contacts from NO and vice-versa?**
  - **FLAG (1 bit): BLE discoverable?**
  - **Service Id: 16byte "Contact Tracing Service"**
  - **(FR) Service data: 16byte "UUID + CountryCode+Timestamp+MAC"**

NO: could possible have 2 services

Backend architecture

Cross-border interoperability

Backend architecture (possible options)

A. Backend federation

- 1/ A NO user in France (respectively a FR user in NO) collects the contact keys.
- 2/ If he/she is diagnosed positive in his/her country, in NO (in FR), he/she uploads the exposed keys to his/her national server. As usual.
- 3/ If he/she is diagnosed positive abroad, in FR (in NO), the national health authority of FR (of NO) requires the national health authority of NO (of FR) to send the required certification to the user, as in step 2.
- 4/ The national server of FR (of NO) sends the NO (FR) exposed keys to the NO (FR) server, on the basis of the country code.

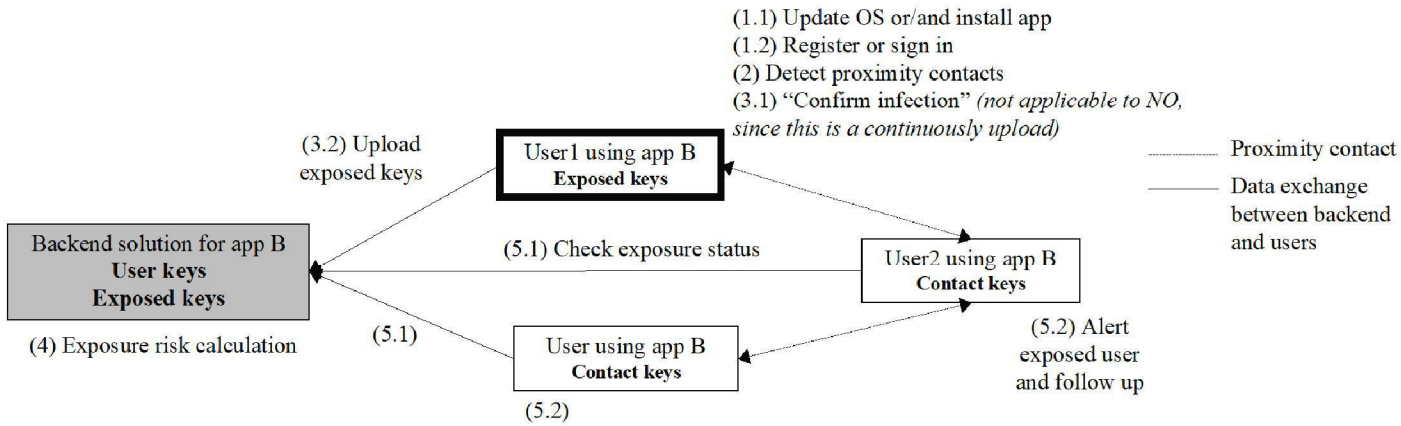
B. Backend federation + forwarding gateway

- **What it is**:
  - One implementation of C/4 (peering between servers) is to use a forwarding gateway for dispatching the appropriate exposed keys to the national severs (NO exposed keys to NO server, etc.).

Steps in the contact tracing flow

Number	Step	Description	Centralised
1	**Enable user with necessary technology**	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	**Proximity contact detection**	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	**Infection confirmation**	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 **[country codes]** **(3.3) Forward to other countries**
4	**Exposure risk calculation**	Exposure risk score is calculated on the server for the exposed contact keys	(4) Exposure risk calculation
5	**Exposure alert and follow up**	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

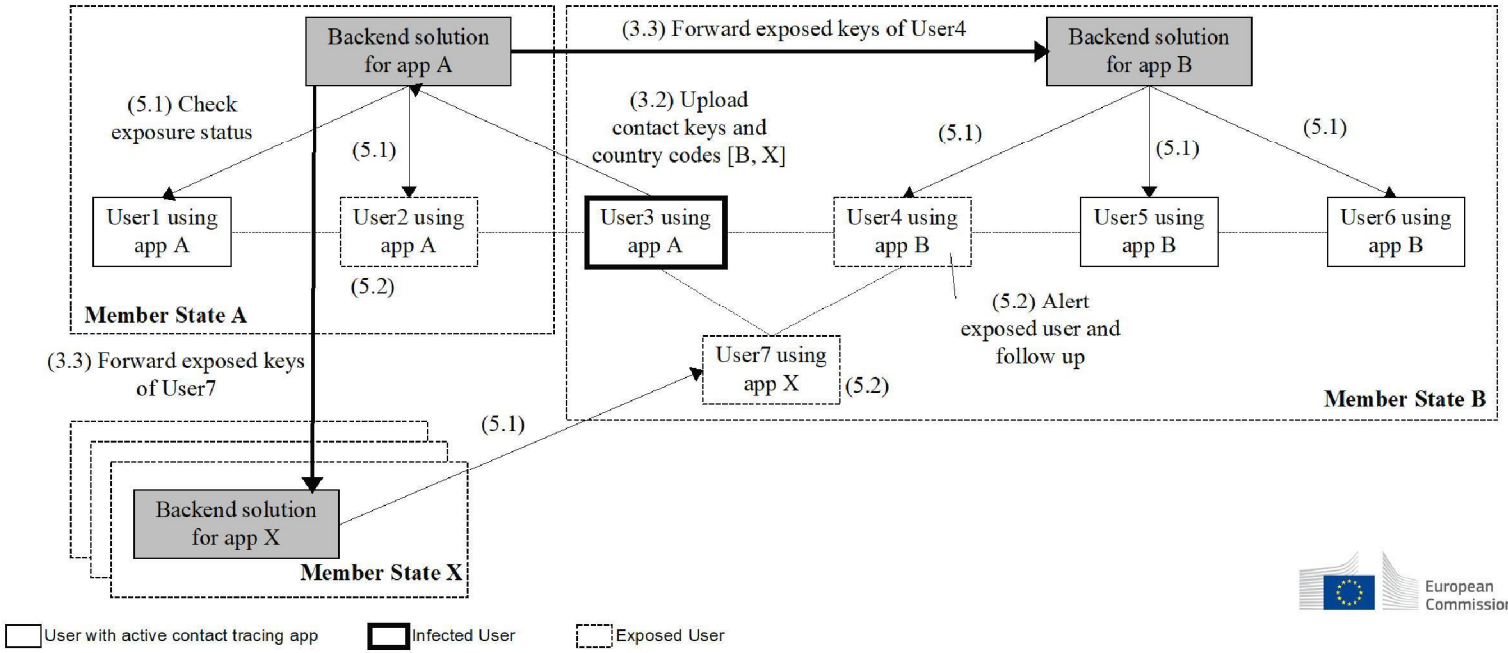
Steps in the contact tracing flow



European Commission

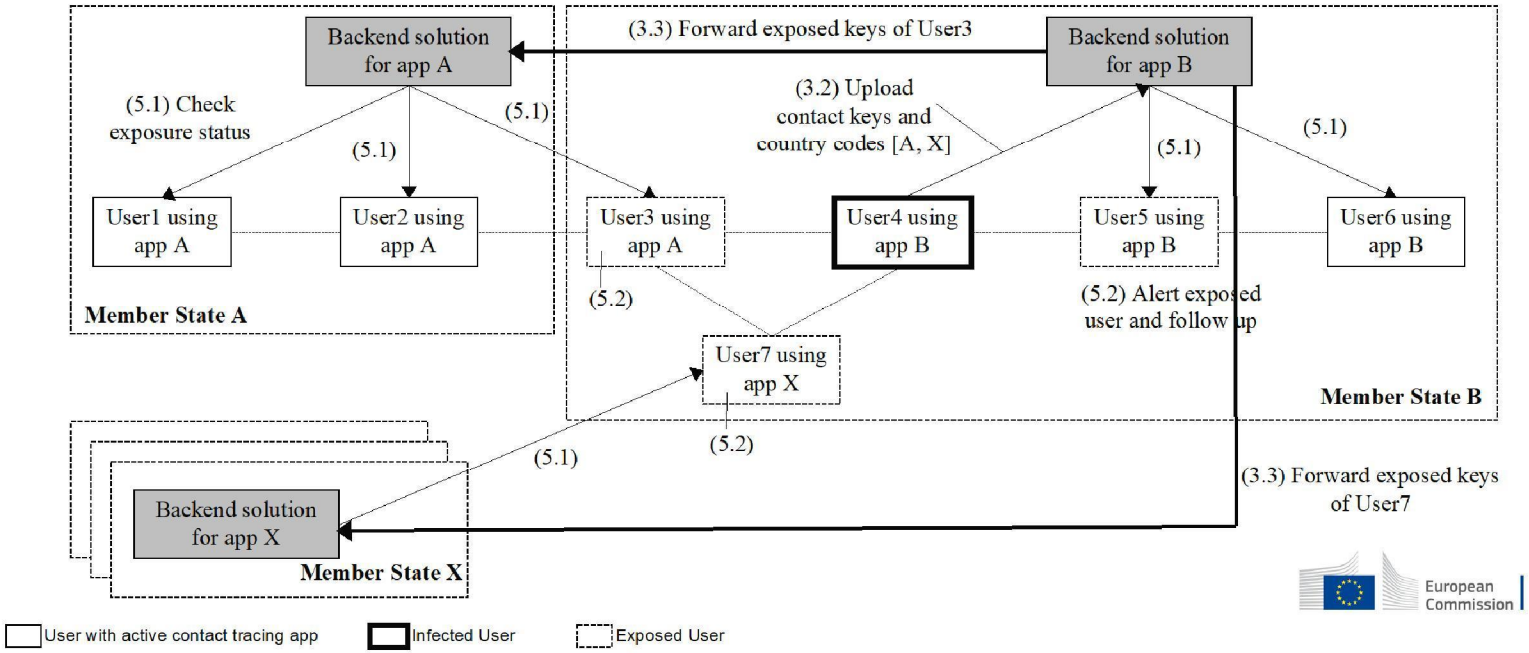
Backend federation

(visiting user infected)



Backend federation

(home user infected)



Next Steps

Next Steps

- **Implementation feasibility assessment [To be confirmed during next meeting]**
  - Next meeting: 29 May – 12:00 (60minutes).

- NOT yet
  - *Share specifications for common components (Bluetooth payloads and backends APIs)*
  - *Aligned implement timeline*
  - *Communications (how to continue liaison, bilaterally or EU cooperation)?*
  - *Legal aspects (bilateral agreement between MS [backend and apps interoperability])*
  - *Foreign user COVID-19 positive test communication to Home Country*