eHealth Network Guidelines

to

the EU Member States and the European Commission

on

Interoperability specifications for cross-border transmission chains between approved apps

Basic interoperability elements

between COVID+ Keys driven solutions

V1.0

2020-06-12

The eHealth Network is a voluntary network, set up under article 14 of Directive 2011/24/EU.
It provides a platform of Member States' competent authorities dealing with eHealth.

Adopted by consensus by the eHealth Network working group on COVID+ keys driven solutions for tracing apps, 12 June 2020

Contents

1 Introduction

Many Member States of the EU (and contracting parties of the EEA) have implemented or plan to implement voluntary and temporary mobile apps that support contact tracing as part of public health strategies to combat the COVID-19 pandemic.

Member States and the Commission agree that these apps should be interoperable so that individual users can be alerted, wherever they are in the EU, if they have encountered a user of another approved app who has been diagnosed positive for the SARS-CoV-2 virus.

This document presents the basic elements for interoperability for "*COVID+ Keys driven solutions*". It aims to keep data volumes to the minimum necessary for interoperability to ensure cost efficiency and trust between the participating Member States. This document is therefore addressed only to Member States implementing this type of protocol.

This document builds on the Common Toolbox, in particular on Section III.6 I.1. on cross-border transmission chains, and the guidelines on essential requirements for interoperability.

2 Definitions

In this document:

- **'user'** means an owner of a smart phone who has downloaded and runs an approved contact tracing app;
- **'reporting/infected user'** means a user who has tested positive for SARS-CoV-2;
- **'exposed user'** means a user who is assessed as having been potentially exposed to a reporting/infected user;
- **'home Member State'** means the EU Member State or EEA country that is responsible for the app supporting contact tracing and exposure notification which the user is using;
- **'home app'** means the approved mobile app of the Member State where the user usually resides;
- **'host Member State'** means a Member State other than the Member State in which the user usually resides;
- **'exposed keys driven approach'** means an approach taken by an app whereby a reporting user informs the app of his/her positive testing and the app uploads his/her proximity contacts to a central backend server; the other users request then the server with a pull mechanism to know if there are at risk;
- '**COVID+ keys driven approach'** means an approach whereby a reporting user informs the app of his/her positive testing and the app uploads his/her temporary keys (i.e. COVID+ keys) to a central backend server which broadcasts them to all other users devices which determine whether an exposure event has taken place;
- **'contact keys'** means unique identifiers broadcasted during proximity encounters between phones that are within radio range;
- **'exposure risk'** means the risk of infection associated with being in proximity to an infected person and the factor that determines whether an alert should be sent to a user;

- **'exposure risk calculation'** means the process to determine the exposure risk (Member States may decide to standardise the exposure risk calculation in line with epidemiological recommendations);
- **'COVID+ keys'** means a subset of unique identifiers from a reporting/infected user;
- **'federation gateway'** means a network gateway that relays, i.e. receives and makes available COVID+ keys' between trusted countries backends;
- **'countries of interest'** means the Member State, or Member States, where a user has been in the last 14 days. This can include the home country and the contries where the user travelled.

3 Basic interoperability elements

This document focuses on basic interoperability elements between solutions that follow an "COVID+ keys driven approach", namely:

1) Bluetooth specification
2) COVID+ Keys
3) List of countries of interest
4) Backend server interoperability
    a. Backend federation
        i. Federation principles
        ii. Basic features of a federation gateway
    b. Connection of the apps with backend servers

3.1 Bluetooth specifications

Devices should have an interoperable way to broadcast and sense proximity with other devices enabled with a contact tracing and exposure notification Bluetooth service.

Following the Bluetooth Specification[1] by Apple and Google, this means to:

1. Broadcast and scan for the *Exposure Notification Service* (for detecting devices proximity), in the 16-bit service UUID section preceding the Service Data section.
2. Include a Service Data section containing two subsections:
    - A *16 byte Rolling Proximity Identifier*: a privacy-preserving identifier derived from the *Temporary Exposure Key* and sent in the broadcast of the Bluetooth payload. The identifier changes about every 15 minutes to prevent wireless tracking of the device.

[1] Version 1.2, April 2020 https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-BluetoothSpecificationv1.2.pdf

- A *4 byte Associated Encrypted Metadata*: a privacy-preserving encrypted metadata that shall be used to carry protocol versioning and transmit signal power for better distance approximation. The *Associated Encrypted Metadata* changes about every 15 minutes, at the same cadence as the *Rolling Proximity Identifier*, to prevent wireless tracking of the device.

3.2 COVID+ Keys

COVID+ Keys, which should correspond to 'diagnosis keys' in the Apple and Google Bluetooth Specifications, are a limited set of *Temporary Exposure Keys* (and their date time information) uploaded to the backend when the device user is diagnosed as positive for the COVID-19.

Temporary Exposure Key is a key that is generated every 24 hours for privacy considerations. This set of *Temporary Exposure Keys* is limited to the last 14 days[2]. If a user remains healthy and never tests positive, their *Temporary Exposure Keys* never leave the device.

The backend server aggregates the COVID+ Keys from all users who have tested positive.

3.3 List of countries of interest

In order to reduce the data downloaded by the user's apps, the apps should be able to identify the countries where a user has been during the past 14 days. If the person has not left its home country, the list will only include one country.

This list can be created following three distinct approaches:

a) device automatic detection of the derived from the NMCC (Network Mobile Country Code)[3];

b) app user manual input;

c) device automatic detection complemented by the app user validation (including the possibility for refinement).

To ensure optimal user experience, a combination of automatic detection and manual validation by the user is recommended.

The list of countries of interest is to:

- be provided to the backend server together with the COVID+ Keys when a user is diagnosed as positive;

- be used by the app in order to fetch the relevant COVID+ Keys from the backend server .

The list of visited countries can be used for data partitioning.

[2] As defined in ECDC guidelines. This number of days may change according to ECDC updates.
[3] Mobile Country Code: https://en.wikipedia.org/wiki/Mobile_country_code

3.4 Backend server interoperability

A federation of backend servers enables the communication of information between countries and ensures that the relevant COVID+ Keys are available to any potentially exposed users.

3.4.1 Backend federation

3.4.1.1 Federation principles

a) Each country should have one backend server, for the purpose of cross-border interoperability;

b) each country backend server should upload all of its own COVID+ Keys and should, in addition, annotate any of these uploaded COVID+ Keys with the (list of) countries of interest for those keys where it considers such relevant.

c) each country backend server should be able to download COVID+ Keys (accompanied by the information about the countries of interest) in available federation gateway.

To facilitate data flow optimisation, the backend servers should make use of the list of countries of interest.

3.4.1.2 Basic features of federation gateway

The federation gateway:

a) is operated by a trusted operator;

b) provides a standardised interface for trusted countries' backends (in the EU/EEA, but also, potentially, in a trusted third country) to upload COVID+ Keys (accompanied by the information about the countries of interest) ;

c) provides a standardised interface for trusted countries backends to download COVID+ Keys (accompanied by the information about the countries of interest) ;

d) has a retention period limited to the minimum necessary so that all trusted countries' backends are able to download all relevant COVID+ Keys;

e) handles only COVID+ keys. No other type of keys can be handled centrally to avoid privacy risks;

f) is open source and auditable.

3.4.2 Connection of the apps with backend servers

Apps should only be able to upload and retrieve relevant COVID+ Keys to and from the home backend server.

4 Implementation

Each country should identify a technical lead who will have operational responsibility for ensure interoperability across Member States.

<u>Stage 1 – Technical specifications/reference implementation</u>

Member States should design detailed technical specifications and reference implementations for:

(1) backend servers and federation gateway;

(2) common functions in contact tracing apps.

Member States, with the support of the Commission, should set up a technical working group with app developers in Member States to implement these activities.

Member States should begin piloting activities for the exchange of keys between countries' backends as soon as possible according the basic interoperability elements presented in this document.

Member States involved in piloting actions should report back to the eHealth Network on the results of these activities.

Member States could also explore the mechanism for confirmation of positive diagnosis for the virus while abroad.

Stage 2 – Federation gateway

A trusted operator for such federation gateway should be selected.

Member States should start piloting exchanges via the federation gateway as soon as it is available.

Stage 3 - Large scale deployment

All Member States running a COVID+ Keys- driven solution should adhere to the specifications finalised during the piloting stages.

5 Security testing and independent review

To ensure transparency, a dedicated group of independent experts can support Member States in the assessment of the apps. Work includes a collaborative platform where facts and opinion are shared, availability of specific tools and practices for assessment, full-cycle technology monitoring, operational support, and a long-term archiving function.

Cybersecurity fora will be mobilised to assess the security aspects of the apps.

6 Conclusions

Digital measures to support the response to the COVID-19 pandemic are being rolled out and will be subject to careful evaluation. Approved, voluntary, mobile contact tracing apps are likely to be downloaded and used by millions of smart phone owners in the coming weeks and months.

Such apps should give those individuals confidence to exercise their right to move freely across the EU, as restrictions are gradually lifted, but only if each of them is fully functional in all Member States that have an approved app. Adhering to the basic interoperability elements described in this document will ensure that apps are interoperable across Member States and work correctly in countries using COVID+ Keys driven solutions.

The Commission stands ready to support this exercise with human and financial resources as necessary.