



Pan-European Privacy-Preserving Proximity Tracing

High-Level Overview

Executive Summary

- Technology can make a significant difference in fighting the current epidemic.
- The solution we provide - PEPP-PT - is designed to help contain the contagion while removing invasive isolation measures.
- PEPP-PT helps to inform and warn people who may be positive of COVID-19, even if asymptomatic, in a quick and scalable way.
- PEPP-PT is a proximity tracing approach, based on Bluetooth Low Energy. The approach excels in privacy protection and international interoperability. It has been developed with the aim of having it adopted by as many European countries as possible.
- PEPP-PT treats privacy with the utmost care. It is compliant with GDPR and adheres to the principles of data minimization and anonymization recommended by the European data protection authorities.
- PEPP-PT is a joint implementation of the PEPP-PT design of national teams of France, Germany and Italy.

Contents

1. Context.....	2
2. Vision and objectives	2
3. Technology Overview	2
3.1 Contact Tracing versus Proximity Tracing	2
3.2 How it works	3
4. Privacy.....	5

1. Context

The whole world is challenged by the need to contain or slow down the spread of COVID-19. The disease is threatening people's health and severely damaging economies on a global scale. The most effective strategy to limit the spread of the virus is to test and isolate COVID-19 cases, immediately inform people who have been in close contact to them, and thereby interrupt infection chains as early as possible. A key challenge is how to identify close contacts at scale, in a privacy-preserving manner. This is where PEPP-PT comes in.

2. Vision and objectives

The PEPP-PT approach is being created by a multi-national European team. Its purpose is to reduce the epidemic's negative impact. In particular, this means:

- Helping to contain the contagion, a prerequisite for saving countless lives and a crucial step towards eradicating the virus
- Minimizing the most radical isolation measures, and accelerating the return to normal, while limiting the risk of new outbreaks

PEPP-PT is designed to address the current crisis with the goal to help to trace infection chains as early as possible and to notify potentially COVID-19 positive people, even if they're asymptomatic. It makes it possible to do so quickly and at scale. This happens in two ways:

1. By warning people who might have contracted the virus but haven't yet been tested.
2. By urging these people act responsively. This may include actions such as to self-isolate and seek immediate medical assistance.

Starting from users proven to be infected by health authorities, reconstructing their trace of proximity events, PEPP-PT warns potentially infected people.

In accordance with our democratic values, we've treated privacy implications with the utmost care. PEPP-PT is in full compliance with GDPR and can also be used when traveling across countries through an anonymous multi-country federation mechanism. No personally identifiable information or location data are collected in the process.

PEPP-PT is designed to be incorporated in country-specific apps to empower them with proximity tracing, thereby integrating this technology into the processes of national healthcare systems and helping them in their COVID-19 response.

3. Technology Overview

3.1 Contact Tracing versus Proximity Tracing

The standard process for identifying contacts is usually carried out by the health authorities (so-called contact tracers) via interviews with the infected patients. This process is very time-consuming and labor-intensive: the contacts are recorded by questioning the infected person who is usually unable to recall contact over the past two weeks without gaps. Furthermore, random contacts (e.g., seat neighbors in public transport) cannot be recorded. The results of this procedure are therefore often incomplete and do not scale.

With the help of PEPP-PT, the process of warning persons who have been in close proximity with a COVID-19 positive subject is accelerated and improved, thus helping to slow down the spread of the

disease. When lockdowns are lifted, the higher efficiency and accuracy could effectively support the healthcare systems and interrupt new chains of transmission as rapidly as possible, containing the infection without jeopardizing society and economy.

3.2 How it works



The figure illustrates the PEPP-PT mechanism for the German implementation.

The PEPP-PT proximity tracing approach uses Bluetooth Low Energy (LE) technology, allowing to notify people at risk with a 90% true positive and 10% false negative rate.

After the user has installed and started the country-specific app that integrates PEPP-PT, the app works in the background - even when the phone is locked - and periodically sends a temporary ID via a Bluetooth LE signal. The temporary ID is generated pseudo-randomly, and changes regularly. It includes the (encrypted) information necessary to map it to a persistent pseudonym of the app that is used to notify it, if needed. In addition to the temporary ID, the signal includes information about the output power of the Bluetooth LE transmission. This serves to estimate the distance between devices accurately.

While working in the background, the app captures the signals of other Bluetooth LE devices that have the app installed. The app keeps a list of their temporary IDs, each representing a contact. For each contact, the duration is determined, and the distance between the devices is estimated. This calculation is possible thanks to the information on the signal output power sent by the transmitting device, and the power as measured by the receiving device.

In contrast to classic Bluetooth, the Bluetooth Low Energy technology requires far less energy and does not drain the smartphone's battery.

Unless a user tests positive to COVID-19, all the temporary IDs collected remain on the user's phone. If a user is found to be positive to COVID-19, a healthcare professional will provide a code that the user inserts into the app. This allows the user to voluntarily send to a server their own list of traced contacts in the form of temporary IDs.

The code created by the healthcare officials is generated pseudo-randomly, is single-use, and changes frequently. This ensures that it cannot be used by malicious individuals to pollute the data collected on the server.

Once the data are obtained from the app of the infected person, the server accumulates the risk of contagion for each temporary ID. This depends on the physical proximity and duration of it with the positive user in the past. The server decrypts the temporary IDs for the users most at risk. The user is informed through a pull or push mechanism. These users receive a notification and get specific information and guidance. This process makes it possible to inform people of their situation much faster and put them in the best position to decide what to do, backed up by advice evaluated by health authorities. Crucially, by isolating and (when the time is right) testing users who contact the health system downstream of our notification, we can reveal many of the asymptomatic citizens who contribute to the virality of the epidemic. This helps to curb the contagion and expedite the return to normality.

4. Privacy

The implementation detailed above is designed to protect the user's privacy rights.

The temporary IDs of the Bluetooth LE devices collected from a particular user's smartphone are generated pseudo-randomly and changed periodically. They do not allow the user even to associate multiple signals to the same device, much less identify the user of the specific device.

In addition, the list of temporary IDs is normally only stored on the device, not sent to the server. Therefore, there is no risk of large-scale data leaks (which, in any case, would not cause serious damage to users, due to the pseudonymization mechanism and the inability of relating persistent pseudonyms to real persons). Moreover, periodically, a data deletion procedure causes older contacts to be deleted.