PEPP-PT

Pan-European Privacy-Preserving Proximity Tracing

# Building Blocks for Pandemic Management Systems using Proximity Tracing

Status: 19. April, 202

## Executive Summary

The purpose of the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) approach is to provide a common basis for a management systems that can be integrated into **national public health** responses to the COVID-19 pandemic. This includes an **operational pandemic management service**, an **operational management planning framework** and an **epidemiological validation service**. These services are implemented on the **operational Pandemic Management Backbone** with the support of the **Pandemic Management Planning Backbone**. Interfaces for integration into national health systems are provided through the **infection verification service** and the **proximity warning service**. PEPP-PT delivers underlying technology which consists of the **smartphone app**, the **proximity measurement**, the **data protection protocol**, the **secure communication protocol** and the **inter-country federation service**.

Contents

# 1 Introduction

The whole world is challenged by the need to contain or slow down the spread of COVID-19. The virus threatens health and severely damages economies on a global scale. The most effective strategy to limit the spread of the virus is to test and isolate COVID-19 cases, to immediately inform individuals who have been in close contact to them, and thereby to interrupt infection chains as quickly as possible. A key challenge is how to identify close contacts at scale, so that—based on this information—the further spreading of the virus can be stopped. This is where PEPP-PT comes in.

The basic functionality of PEPP-PT is to accelerate the building of interoperable national apps in order to more quickly and precisely warn individuals who may be at risk of a SARS-CoV-2 transmission using ubiquitous digital technology. The necessity for such a mechanism arises, because manual contact tracing is too slow and incomplete to warn individuals before they might transmit the virus [1].

# 2 Criteria for Success of PEPP-PT

However, the use of this proximity measurement mechanism for a successful pandemic management system is a very complex matter; it depends on usage by a sufficiently large percentage of the population. The strong measures currently in place—lockdown of entire social and economic systems—are unsustainable for society and economy. In the current epidemiological situation, most health authorities will develop strong mitigation measures; that is, they will limit the spread of the virus by testing, isolating positive subjects, identifying contacts, and recommending quarantine.

What makes SARS-CoV-2 infection chains hard to trace is the fact that infected persons are contagious before they show symptoms of infection. Therefore, tracing infection chains means that contact persons need to be determined some days after the contact has happened. A key challenge is: how do we inform exposed contacts at scale? Because time is short, a hardware basis is required to support proximity measurement and to enable proximity tracing.

There are a number of wireless distance measurement mechanisms that include time of flight, radar, ultrasound, or radio signal strength. Except for the last two mechanisms, the specialized hardware necessary for efficient proximity tracing is not available in sufficient numbers to achieve the goal of proximity tracing.

**Smartphones**, however, are a ubiquitous digital technology. In most European countries, at least 70% of the population possesses a smartphone. These smartphones can be retrofitted as measurement devices; the proximity of two phones over a longer period of time can be determined through their Bluetooth technology. These measurements can be mapped into a warning that can be communicated to individuals at risk, so that—based on this information—the further spread of the virus can be stopped.

However, smartphones are highly personal devices and typically contain large amounts of personal data. Hence, integrating proximity measurements with a mechanism to warn the person who owns the phone in close proximity depends on a high acceptance and trust among large parts of the population. In European democracies, this can be achieved by the following mechanism requirements for which PEPP-PT provides an interoperable level playing field—similar to a standardization body—for the national systems, on the basis of the joint description for associated mechanisms and services.

| **Requirement** | **PEPP-PT mechanism** |
|---|---|
| Voluntary and will be dismantled as soon as no longer needed | **(1) Smartphone app** can be installed and deinstalled without any legal consequences and all data will be deleted |
| Approved by the national health authority with a secure and trusted mechanism to validate infection status | **(2) Infection verification service** will assure that the test result is immediately conveyed and that users at risk are immediately warned |
| Will be voluntarily warned and acts responsively | **(3) Proximity warning service** |
| Ethical and efficient balance between epidemic risk reduction, the freedom of individuals, and economic considerations when implementing the national public health response | **(4) National health policy framework** |
| Based on the national health policy framework and the most advanced scientific results and data | **(5) Pandemic management planning framework** |
| Validated effectiveness of the pandemic management system | **(6) Epidemiological validation framework** |
| Operated in a secure and trusted backbone | **(7) Operational Pandemic Management Backbone** |
| Transparent planning of pandemic backbone operation based on ethics, data, and science according to national public health policies | **(8) Pandemic Management Planning Backbone** |
| Process is conducted by country/region of user registration | **(9) Inter-country Federation Service** |
| Privacy-preserving | **(10) Data Protection Protocol** |
| Secure | **(11) Secure communication protocol** |
| Proximity measurement for smartphones | **(12) Bluetooth-based proximity measurement** |

Components (1) - (12) are the functional building blocks of PEPP-PT and will be described in more detail.

# 3 Functional Building Blocks for Pandemic Management

Using proximity-tracing technologies for effective pandemic management requires several functional building blocks to work in conjunction. These functions comprise, for instance, proximity measurements using standard smartphone hardware, transport protocols, verification of infection status in coordination with the public health system, and a pandemic management service. **Error! Reference source not found.** illustrates the main building blocks that are believed to be required to effectively trace and stop infection chains.

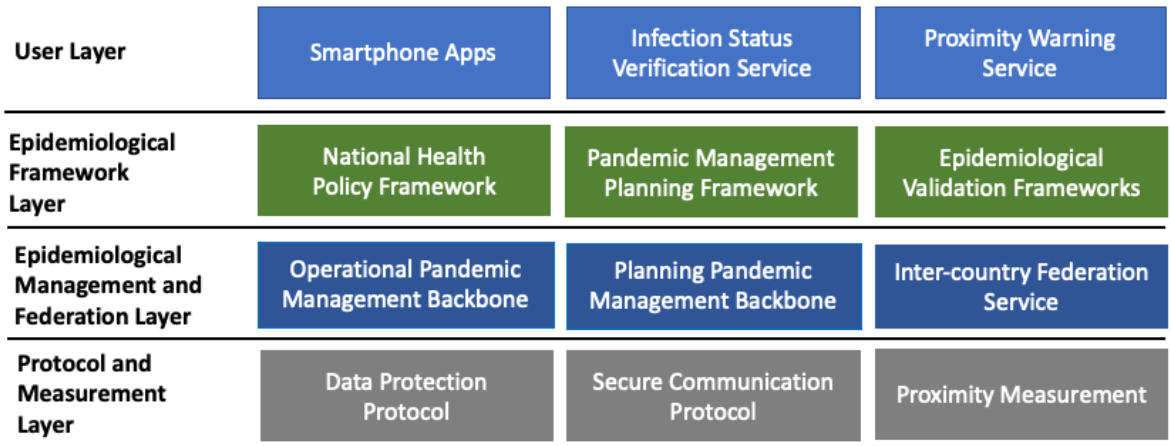


*Figure 1: Functional building blocks of a pandemic management system based on proximity tracing.*

## 3.1 Smartphone App

The PEPP-PT functionality of the system is delivered to users in the form of a smartphone app. The app serves as the user's device to determine proximity to other PEPP-PT phones. The interactions to verify a user's infection status and to notify other users about proximity events that may have been an exposure risk are also performed through the app.

## 3.2 Infection Verification Service

The approval of the pandemic management system by the national health authority is needed in order to provide a secure and trusted mechanism to validate infection status. This way, a user is informed about the result of the test.

Given this secure information, index cases that have been deemed positive can activate the proximity tracing mechanism. The pandemic management system can then inform those at risk very swiftly, so that these individuals can immediately take appropriate measures including self-isolation. This is an effective means to stop infection chains.

However, were it possible for individuals to misuse the system with a fake infection status, this would have a negative impact on society and the economy. Therefore, each pandemic management system needs to include an infection verification service, which checks whether

or not a user's infection can be confirmed. Only in confirmed infection cases may those contacts be notified to self-isolate

Verification of the infection status of users can be best performed if this information is available from the public health system. Therefore, it is recommended to develop a solution that is integrated with the information technology systems of public health authorities to enable reliable infection status verification.

Moreover, it should be considered to offer a secure mechanism for individuals who experience symptoms of COVID-19 to activate the warning of their contacts.

More globally, the infection verification service will most likely be country-dependent.

After a user with a validated infection status has uploaded the proximity measurement data form the phone, the proximity measurement is disabled, to prevent quarantine surveillance approaches.

### 3.3 Proximity Warning Service

Based on a risk score, a possible contact of an index case receives an encrypted and anonymized notification message and will be informed about the possible exposure. From there, the voluntary operational follow-up process with the health authorities can be conducted, which will typically be country-dependent.

At no point should any PEPP-PT-based system be used to monitor the behavior of infected individuals or those at risk. That is, the privacy-preserving characteristics do not end with notification, but are maintained in the periods after the notification (i.e., PEPP-PT provides no means through which a government—or anyone else—can control or monitor at-risk individuals).

### 3.4 National Public Health Policy Framework

It is the responsibility of national public health authorities to coordinate the national public health response in an ethical and transparent framework. Public health authorities will coordinate the local proximity-tracing process in line with national and international guidance, which defines those contacts who should be warned and how those contacts should be managed.

Ethical and efficient pandemic management requires adjustment and fine tuning of the various pandemic management measures. Infection risk scoring needs to be adjusted for an ethical and **transparent** balance between epidemic risk reduction, freedom of individuals, and economic considerations.

### 3.5 Pandemic Management Planning Framework

Managing public health intervention is an iterative and empirical process. Decisions need to be made and adjusted based on experience and the state of expert knowledge and science following the national public health policy. Therefore, a pandemic management system

should include a pandemic management planning framework, which allows health authorities to apply pandemic management policies appropriate for the current situation.

The fight against the SARS-CoV-2 pandemic involves ongoing scientific research dedicated to better understanding the infection paths and risk factors of this virus. Epidemiologists are constantly developing their knowledge about SARS-CoV-2 and infection models. Through new research data, epidemiologists will iteratively refine their models, which can then be applied to infection risk scoring and pandemic management.

Moreover, as public acceptance is a necessary requirement for the system to fulfill its purpose, it should be based on the most advanced science. Hence, analyzing research data is another building block of effective pandemic management planning.

### 3.6 Epidemiological Validation Framework

Public health authorities must assess the effectiveness of the approach. This can help public health authorities tailor prevention efforts and also help them understand whether the infection risk scoring based on proximity and time duration measures needs to be adjusted. The epidemiological validation service should also statistically assess the accuracy of applied models. This validation is a necessary justification for why proximity tracing is in conformance with General Data Protection Regulations (GDPR).

### 3.7 Operational Pandemic Management Backbone

The system should be operated in a secure and trusted backbone, which can be easily deployed locally or used from an external provider if local provisioning is not possible in time. The backend must be well tested and able to handle hundreds of millions of interactions to ensure that the device network and interaction with the health authorities are completely reliable and scalable.

### 3.8 Pandemic Management Planning Backbone

Transparent planning of a pandemic operation based on ethics, data, and science according to national public health policies will also be operated in a secure and trusted backbone. All relevant data, including donated research data, will be processed to advance the scientific understanding of the virus and epidemiological development. Simulations will be conducted for the planning of adjustments of the operational pandemic backbone.

### 3.9 Inter-Country Federation Service

During normal times, individuals travel between different countries. Particularly in Europe, citizens can move freely within the Schengen Area without border controls. During the SARS-CoV-2 pandemic, borders have been closed to contain the spread of the virus. To reopen borders and allow the free flow of individuals and goods, proximity-tracing systems need to work inter-operably across borders.

Although pandemic management systems are to be implemented on the national or regional level, such systems need to function in a federated mode to allow tracing of infection chains across country borders. Hence, a mechanism is required to identify from which country or region's server a particular EBID has been logged for a PEPP-PT. As a privacy requirement, the mechanism needs to be encrypted so that it cannot be retrieved by inspecting the EBID.

### 3.10 Data Protection Protocol

The usage of proximity-tracing systems needs to be voluntary, privacy-preserving, and in full compliance with highest data protection standards, such as the European GDPR.

A pandemic management system using proximity tracing needs to preserves privacy of users and ensures health data is protected and treated with utmost care. Users should be able to stay anonymous or pseudonymous and thus able to use the service without revealing their real identity.

### 3.11 Secure Communication Protocol

Proximity-tracing systems as described above are distributed systems, comprising user end devices (smartphones) and central services. Such systems need a secure communicate information between end devices and central services. The transport layer needs to rely on secure data transport protocols to ensure integrity and confidentiality of such data.

### 3.12 Proximity Measurement

SARS-CoV-2 is mainly spread via droplet infection. Current epidemiological models assume a distance of less than 2 meters over a time of 15 minutes to put individuals at an increased risk of infection. The duration and type of interaction between individuals also have a high impact on the infection risk, but are very difficult to measure using the chosen measurement tools.

Measuring the proximity to other individuals while both individuals are unaware of whether they are infected is a key requirement of proximity-tracing systems. Today, this can be achieved with Bluetooth Low Energy (BLE) technology that is built in standard smartphone hardware. Although BLE has been built to transmit data, the radio signal strength can also be used to measure proximity.

After a user with a validated infection status has uploaded the proximity measurement data from the phone, the proximity measurement is disabled to prevent quarantine surveillance approaches.

## 4 Alternative End User Devices

There are individuals who do not own a smartphone. This includes individuals under the age of 10 and above the age of 70. In these instances, there should be an alternative solution to enable participation in the proximity-tracing system: special proximity-tracing devices, which perform the same functionality as smartphone apps. Hence, future work will be devoted

towards developing specialized devices that can be integrated into the PEPP-PT approach. These devices will be specialized and provided to individuals who do not own a smartphone.

# 5 References

[1] L. Ferretti, C. Wymant, M. Kendall, L. Zhao, A. Nurtay, L. Abeler-Dörner, M. Parker, D. Bonsall and C. Fraser, "Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing," *Science,* 31 April 2020.