

# ROBERT: ROBust and privacy-presERving proximity Tracing<sup>1</sup>

Inria, France<sup>2</sup>  
Fraunhofer AISEC, Germany

April 18, 2020

## Proximity Tracing applications

The COVID-19 virus is hard to trace because many people can be carriers, and therefore be contagious, without knowing and before experiencing any symptoms. Hence, COVID-19 virus carriers may transmit it to many other people in their vicinity.

The main goal of proximity tracing mobile applications is to notify people that they have been in close proximity to COVID-19 virus carriers even if these carriers were not even tested at the time of interaction.

In this context, it is possible to take advantage of Bluetooth, a wireless technology available in modern smartphones that is used for exchanging communications among devices over short distances. Bluetooth is therefore able to detect when users are in close proximity and an application can use it to allow users to know that they have been exposed to COVID-19 virus carriers. Ensuring the highest data protection and security standards would encourage a quick and broad adoption of such an application by citizens. In this document, we propose a solution - the [ROBust and privacy-presERving proximity Tracing \(ROBERT\) scheme](#) -- that can be used to build proximity tracing mobile applications.

The ROBERT protocol is a proposal for the [Pan European Privacy-Preserving Proximity Tracing \(PEPP-PT\)](#) initiative, whose main goal is to enable the development of contact tracing solutions respectful to the European standards in data protection, privacy and security, within a global response to the pandemic.

## Security and privacy considerations

Proximity tracing applications should provide the most useful functionalities to limit the spread of the virus in a robust, secure, and reliable way. Another key factor influencing the adoption of these applications is to ensure the protection of the privacy of its users. These requirements are essential to justify the legitimacy of their deployment and their acceptability by citizens who should be free to install them as well as to uninstall them at any time. We do not discuss the effectiveness of these proximity tracing applications here, as it has to be parameterized and assessed in collaboration with epidemiologists. We rather focus on security and privacy issues.

---

<sup>1</sup> This document is aligned with ROBERT Protocol technical specification version 1.0:  
<https://github.com/ROBERT-proximity-tracing>

<sup>2</sup> Collaborative Inria work led by the PRIVATICS team.

To protect user's privacy, proximity tracing applications should follow the data minimisation principle of GDPR, and only collect the information required to achieve the main purpose of these applications: notifying users that they have been in close proximity of COVID-19 virus carriers. In particular, proximity tracing applications should not collect any geolocation data; instead, they should rely on the collection of temporary pseudonyms.

Proximity tracing applications should provide the highest privacy standard for their users, and protect them from the central authority, from other users and from other malicious third parties. Most importantly, such applications should not be turned by users into a spying system especially to learn whether people living or working in a specific location are diagnosed with COVID-19 or not.



These applications should be resilient to attacks and work even in the presence of malicious users who want to interfere with or break the functionality of such applications.

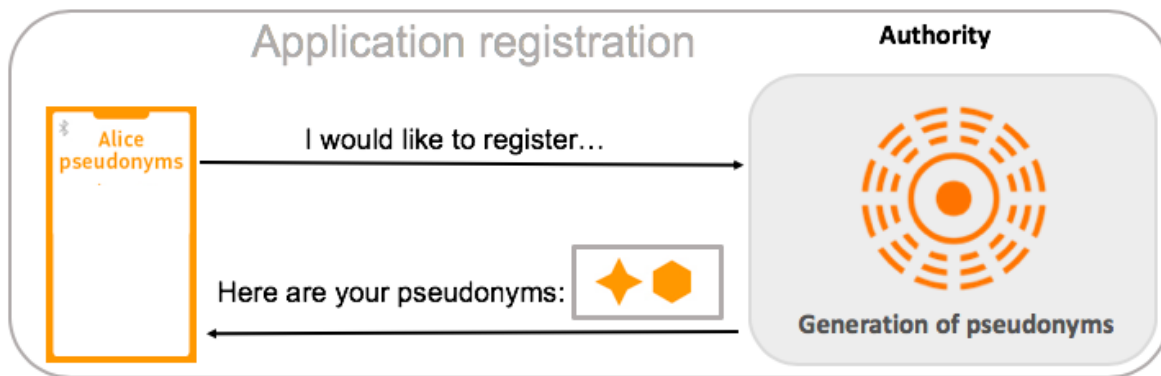
These applications should also include a mechanism to ensure that they are disabled as soon as they are not needed, i.e., at the end of the pandemic, or on the request of their user.

## ROBERT: ROBust and privacy-presERving proximity Tracing protocol

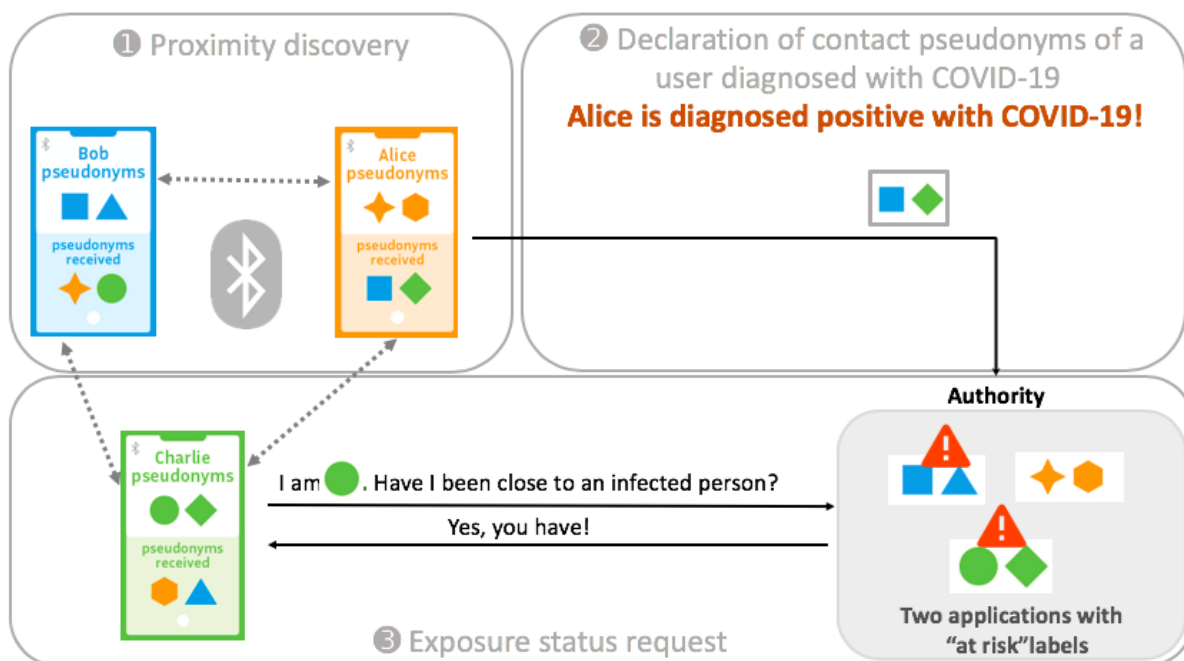
We propose the ROBust and privacy-presERving proximity Tracing (ROBERT) protocol that can be used by proximity tracing applications. To detect whether two users have been in proximity to each other, the applications rely on short-range communications exchanged using the Bluetooth wireless technology activated on both users' devices.

The user voluntarily installs a mobile application that uses ROBERT on his/her smartphone. Upon installation, the application registers with the central authority. This authority generates and shares a set of temporary pseudonyms with the user's application. We can think of these pseudonyms as temporary "fake names" associated with the user's application. In practice, these pseudonyms look like random numbers; in this document, for the sake of simplicity, we will use geometrical shapes.



As a simplified illustration, for user **Alice** in the figure below, the application receives several pseudonyms for her -- here  and  -- that will be used one after the other. This is meant to protect Alice's privacy and ensure that no external observer or user of the application can link these pseudonyms to track her over time. The pseudonyms of a user can only be linked by the user himself and the authority.





There are three main phases of the protocol: proximity discovery, declaration of contact pseudonyms of users diagnosed with COVID-19, and exposure status request.



## ① Proximity discovery

The mobile application of **Alice** relies on short-range communications using Bluetooth to “announce” one of her pseudonyms -- either  or  in our example -- to any other user who is in close proximity to **Alice**. In the example above, **Alice**’s application announces her presence to the applications of **Bernard** and **Charles**.

In the figure above, the mobile application of each user, **Alice**, **Bernard** and **Charles**, relies on short-range communications using Bluetooth to collect all the pseudonyms of users that are nearby. The mobile application then records these pseudonyms *locally on the user's smartphone*. In our example, **Alice** has met **Bernard** and **Charles** and, hence, their pseudonyms,  and , are stored on Alice’s smartphone.

## ② Declaration of contact pseudonyms of a user diagnosed with COVID-19

If **Alice** gets tested positive for COVID-19, to help people who have been around her in the last 2 weeks, she agrees to anonymously communicate their pseudonyms (■ and ◆) to a central authority. The central authority receives these pseudonyms **without any information** about **Alice**. Therefore, **the authority learns neither pseudonyms nor real names of users diagnosed with COVID-19**. Each time the authority receives a pseudonym of contacts of some users diagnosed with COVID-19, it associates a special “at risk” label to the application corresponding to the registered pseudonym. In our example, **Bernard** and **Charles**’ applications are now labeled with a warning “at risk”.

## ③ Exposure status request

To check whether **Charles** has been in close proximity to users diagnosed with COVID-19 in the past several days (for example, two weeks), **Charles**’ application sends his current pseudonym, say ●, to the central authority. The central authority finds the registered application corresponding to this pseudonym and checks whether it is labeled as “at risk”. Note that the authority cannot identify the users that these pseudonyms represent; this information does not exist.

If the authority finds that the registered application is marked as “at risk” (which is the case for **Charles**), the authority responds to the user’s request by informing him he has been in close proximity to users diagnosed with COVID-19 and, hence, he has been exposed to COVID-19. Otherwise, the authority informs the user that he has not been exposed as far as the authority can tell.

---

—

## Frequently Asked Questions

### General questions

Q: Is “ROBERT” a smartphone application?

No, ROBERT is not an application. It’s a communication protocol -- that is to say a procedure describing how an application should work. It is proposed by scientists who have been working on security and privacy of communication protocols for more than 20 years. Different applications can use the ROBERT Protocol.

ROBERT is proposed in the context of the Pan European Privacy-Preserving Proximity Tracing (PEPP-PT) initiative, which main goal is to ensure that the European standards in data protection, privacy and security are respected by proximity tracing protocols and applications.

## Privacy and security concerns

Q: Can this application be used by the central authority for tracking me or conducting mass surveillance?

In order to “track you”, two types of information should be collected: (1) your identifier (to detect you are the same person that has been seen before) and (2) some personal information about you. In ROBERT, the authority receives some information only during the phase when pseudonyms of contacts of a user diagnosed with COVID-19 are sent, and the authority receives only a user’s pseudonym during the “exposure status request” phase. In addition, only a temporary pseudonym is used, and the only information the authority can derive from such pseudonym is that the corresponding person has been exposed (i.e., in proximity to a user diagnosed with COVID-19). Therefore pseudonyms do not allow the authority to track users.

The authority does not learn the real identities of any user, whether diagnosed with COVID-19 (i.e., tested positive), such as Alice above, or exposed, such as Bernard and Charles. Also, the authority cannot infer the “proximity graph” of Alice, Bernard or Charles. If the authority wants to do physical tracking, it will need to deploy sniffing devices or compromise the user’s mobile device by exploiting a vulnerability on his phone, which could lead to targeted surveillance but not mass surveillance. In addition, this kind of physical tracking is already feasible with other solutions such as video-surveillance, GSM boundary, or dedicated tracking devices.

Q: I walked past a person on the street. Can I know whether or not that person is diagnosed with COVID-19?

No, you cannot. Knowing **whether or not the person is diagnosed with COVID-19** would violate her privacy. The ROBERT protocol ensures that when a user tests positive, her application gets disabled, and the person can be asked – by her health professional (doctor/general practitioner) – to self-isolate for two weeks. When she recovers, her health professional will re-enable her application.

Q: If I test positive, who can learn if I have been diagnosed with COVID-19?

Only health professionals who have access to your test results will learn that you have been diagnosed with COVID-19. Neither the central authority nor users of the application will have access to your test results. Also, they will not be able to infer who is and who is not diagnosed with COVID-19.

When a user receives the following message: *"You have been in close proximity to people diagnosed with COVID-19"*, and that user has been in contact with very few people (in our example, Charles has been in close proximity to Alice and Bernard), the user could guess that one of these people is diagnosed with COVID-19. If this risk is deemed unacceptable, the ROBERT protocol could be enhanced with a probabilistic mechanism to protect infected users from such guesses. The choice of such options is currently strictly out of the ROBERT Protocol specification.

Q: How are my pseudonyms generated? Can someone use my pseudonym? Is it secure?

Ephemeral pseudonyms are generated by the authority using a secure cryptographic function applied to a secret key associated with your application and timing information. These ephemeral pseudonyms are then sent securely to your application and stored for future usage. Only the authority and your application can access them. Ephemeral pseudonyms are then broadcast on Bluetooth to inform nearby applications. To limit the risk that the message containing your pseudonym be reused by a malicious user, this message is only valid during a few seconds (what we call "replay protection").

Q: How does ROBERT protocol ensure that the central authority does not associate my pseudonyms with me?

All your pseudonyms are known by the authority (since the authority generated them). However, the authority has no additional information (e.g., name, address, phone number, smartphone technical identifier or geolocation) that could be used to identify you.

Q: How can I ensure that all interactions with the authority are secure, and the response that I receive from the authority (whether or not I have been exposed to users diagnosed with COVID-19) is reliable?

The installation of the application involves a registration phase in which a secret key is generated and shared between the user's mobile device and the authority. The key is then used to generate ephemeral pseudonyms and to digitally sign the messages exchanged with the authority. Digital signatures are mathematical schemes used to verify the authenticity of messages. It gives the recipient a very strong reason to believe that the message was created by a known sender, and its content has not been altered in transit. Moreover, communications between the application and the authority are all encrypted.

## Functionality of applications that implement the ROBERT protocol

Q: What kind of information will be sent in the alert message (recommendations, mandatory instructions)?

The ROBERT protocol is designed to enable the application to notify the user if she has been in close proximity to individuals diagnosed with COVID-19. Following the status request sent by the application to the authority, the user will receive a response to her request (or an alert message) informing her whether or not she has been in close proximity to users diagnosed with COVID-19. The type of instructions that will be transmitted as well as how often that information will be shown on the user's mobile phone depend on the health professional and epidemiologists decisions.

Q: Can I learn from the alert message whether or not I have been in close proximity to a user diagnosed with COVID-19 in the past x days?

The current protocol is designed to return a "binary" answer: either "Yes, you have been in close proximity to one or more users diagnosed with COVID-19 in the past x days" or "No, as far as we can tell, you have not been in close proximity to a user diagnosed with COVID-19 in the past x days." The number of days 'x' will be defined by the health professionals and epidemiologists.

Q: How long do I have to interact with a person diagnosed with COVID-19 to be considered later as potentially infected? How close should I be?

These choices are not fixed and will be chosen in agreement with health professionals and epidemiologists.

## Accessibility by population

Q: Would people who do not own smartphones, such as children, be able to use this system?

Indeed, people who do not own or can't use a compatible smartphone would not be able to benefit from a proximity tracing application if it is available only on smartphones. However, it may be possible to create a device which emulates the application functionalities and which could be used by user groups who have specific needs. This option is currently being investigated.

Q: How can those who lack technical skills to download and use the app?

The app will be as simple as possible to ensure that lack of technical skills is not an obstacle to adoption. People who do not possess these skills could seek help from a relative or a caretaker. Otherwise, a dedicated device that works out-of-the-box (see previous question) could be provided.

## Bluetooth functionality

Q: Is Bluetooth transmission secure? Can someone eavesdrop on me?

The Bluetooth communications used by the system cannot guarantee confidentiality: anyone can read them. However, the data exchanged over Bluetooth is limited to the temporary anonymous pseudonym, the transmission time, and an integrity verification code. This information is used to protect against replay attacks (when the message can be captured and re-sent later by the attacker in an attempt to impersonate the user): this attack will not be feasible.