DESIRE: A Third Way for a European Exposure Notification System[1]

Leveraging the best of centralized and decentralized systems

Nataliia Bielova[2], Antoine Boutet, Claude Castelluccia, Mathieu Cunche,
Cédric Lauradoux, Daniel Le Métayer, Vincent Roca
PRIVATICS team, Inria, France
desire-contact@inria.fr

May 9th, 2020

A purpose: building a third way that leverages the best of the centralized and decentralized systems

The COVID-19 virus is hard to trace because many people can be contagious, without knowing and before experiencing any symptoms. Once a person is tested positively with COVID-19, the health workers perform "contact tracing" asking the infected person to provide information about all the people she has been in close contact with. However, such manual contact tracing does not work well if the infected person has been at crowded places, such as supermarkets and public transports, and therefore has been close to many people she does not know.

The main goal of an exposure notification application is to complement manual "contact tracing" and to inform 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.

Currently, two protocol families exist in Europe: the so-called "centralized" protocols (that rely on the transmission of "exposed" pseudonyms, from the application of a person diagnosed positive to a central server) and the so-called "decentralized" protocols (that rely on the transmission by a central server of the pseudonyms of persons diagnosed positive to all the smartphones). These protocols each have advantages and drawbacks, in terms of robustness to attacks (carried out by the central authority or by users), in terms of control by the Health Authority. because of the different nature of data, they cannot easily interoperate.

This document presents the another way to leverage the best of the two approaches, with the goal to have an interoperable protocol in the mid-term at the European level : the DESIRE protocol – a decentralized evolution of *the ROBust and privacy-presERving proximity Tracing scheme (ROBERT)*. There are two major improvements brought DESIRE:

1. While ROBERT relied only on temporary pseudonyms for users' applications, DESIRE relies on *"Private Encounter Tokens"* (PETs) that associate a unique and secret pseudonym exclusively during an encounter between two mobile devices that were in proximity to each other. PET tokens are *generated jointly and privately by the applications of these two users*

[1] This document is aligned with DESIRE Protocol technical specification: https://github.com/3rd-ways-for-EU-exposure-notification/project-DESIRE

[2] Nataliia Bielova is the contact author. All the other co-authors are listed in alphabetical order.

and are unforgeable, thus providing a high level of privacy protection. This generation local to the applications is a significant form of decentralisation.

2. All the data that is stored by the central authority is now encrypted with the secret keys that are stored on users' devices, thus providing a strong protection against data breaches.

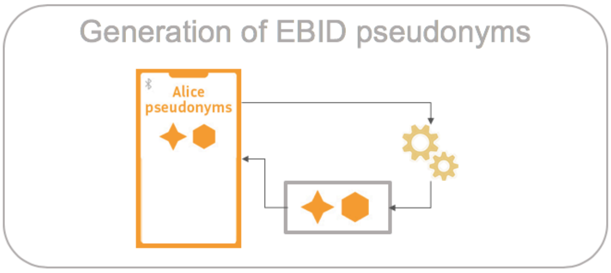
These new features improve drastically the privacy guarantees of DESIRE scheme with respect to the authority or malicious users.

The local generation of PET encounter tokens enables to benefit from the guaranties associated to decentralized solutions towards a malicious central authority. Just like ROBERT, DESIRE gives a full control to the health authority (for regulation and knowledge) in terms of management in the context of a global health strategy : it relies on a central authority to compute the "risk score" – a score that determines the exposition level of the user to COVID-19. With the help of epidemiologists, the epidemic can be monitored in real time in order to dynamically adjust the algorithm that computes the "risk score". Indeed, a key success factor of proximity tracing applications is their smooth integration within the existing health care infrastructure, in particular the possibility to adapt this "risk score" to the local epidemiological situation and the available resources.

DESIRE: Protocol Overview

Upon installation, the application registers itself with the central authority, that creates an entry in its database. This registration process uses anonymous authorization tokens and is designed in a way to preserve the user privacy. The registration process also guarantees that only one application is used by each device, which helps to prevent certain types of attacks.

After successful registration, the application periodically generates new temporary pseudonyms, called *"Ephemeral Bluetooth Identifiers",* or EBIDs. We can think of them as "nicknames" 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.

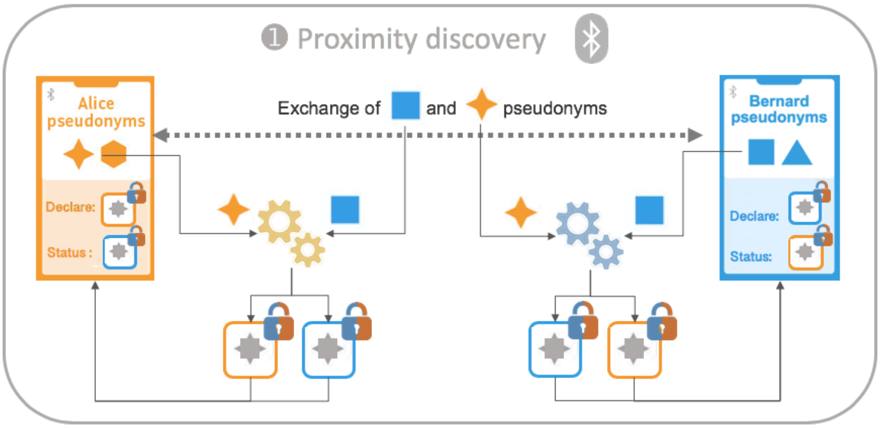


As a simplified illustration, for user **Alice** in the figure above, *the application periodically generates EBID pseudonyms* – here ✦ and ⬢ – that will be used one after the other. These pseudonyms are meant to be broadcasted to all the mobile devices around Alice, but they will never be communicated to the central authority: they only have a local and temporary use (their usage is limited in time).

The protocol features three main phases, presented below: proximity discovery, declaration after a positive test, and exposure status request.

❶ Proximity discovery

The mobile application of **Alice** relies on short-range communications, Bluetooth, to “announce” her current pseudonym – either ✦ or ⬢ in our example – to all users who are in close proximity to **Alice**. In our example, **Alice**’s application announces her presence to **Bernard**’s application.



Each mobile application collects all the pseudonyms of users that are nearby. To ensure that only **Alice**’s and **Bernard**’s applications record each other’s proximity, DESIRE protocol relies on the well-known Diffie-Hellman scheme: with this cryptographic scheme, **Alice**’s and **Bernard**’s applications generate a shared secret between them called *“Private Encounter Tokens”* (PET tokens, showed with ▣ and ▣ symbols) from their respective EBIDs.

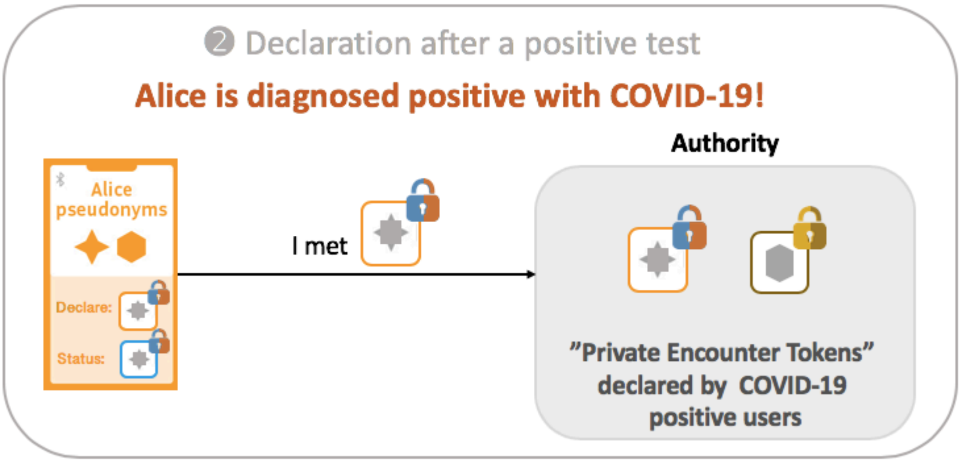
Alice’s application will use the orange token ▣ during phase ❷ of the protocol to declare her encounters in case she turns out to be COVID-19 positive – this token is stored under “Declare” list on **Alice**’s mobile device. The blue token ▣ will be used to request her exposure status during phase ❸ of the protocol – this token is stored under “Status” list on **Alice**’s mobile device.

Bernard’s application will generate the same two PETs, but will use them in a reversed order: the blue token ▣ to declare his encounters and the orange token ▣ to request his exposure status.

These two PET tokens are only known to **Alice** and **Bernard**, stored locally on their mobile devices and no other party can link them with either **Alice**’s or **Bernard**’s pseudonyms. Moreover, no party can link the orange and blue tokens with one another.

❷ Declaration after a positive test

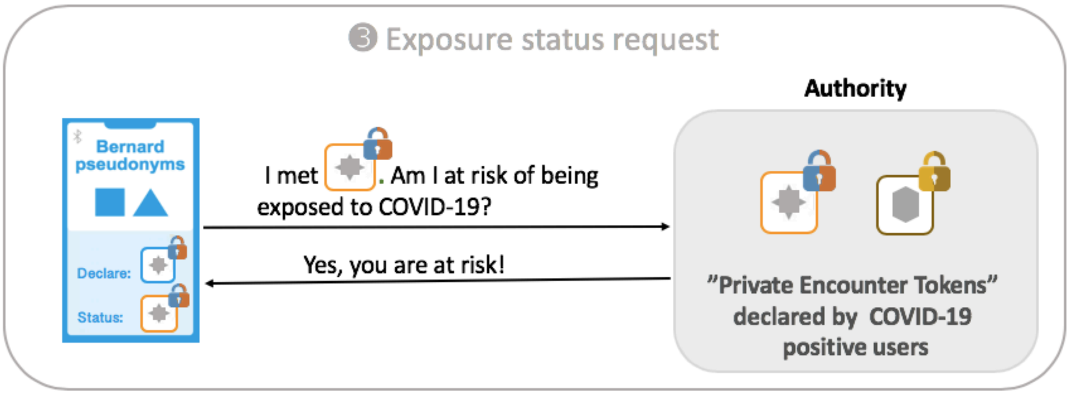
Alice gets tested positive for COVID-19. To help people who have been around her during a contagious period, she agrees to anonymously communicate the PET tokens from the “Declare” list (hence, only the orange token) generated by her application to the central authority.


❷ Declaration after a positive test
Alice is diagnosed positive with COVID-19!
Alice pseudonyms
Declare:
Status:
I met
Authority
"Private Encounter Tokens" declared by COVID-19 positive users

In case Alice has one or more PET tokens in her "Declare" list, the central authority receives these PET tokens *independently without any information* about **Alice**. Therefore, *the authority learns nothing about the users, in particular no pseudonyms of users tested positive for COVID-19, and is not able to link these PET tokens together to create their "proximity graph".* Each time the authority receives a PET token, it stores this token in a list of tokens.

❸ Exposure status request

To check whether **Bernard** has been in close proximity to users diagnosed with COVID-19 in the past several days (for example, two weeks), **Bernard**'s application provides all his PET tokens from his "Status" list to the central authority. The central authority checks whether **Bernard**'s PET tokens are present in the global list of tokens that indicate proximity to users diagnosed with COVID-19.


❸ Exposure status request
Bernard pseudonyms
Declare:
Status:
I met . Am I at risk of being exposed to COVID-19?
Yes, you are at risk!
Authority
"Private Encounter Tokens" declared by COVID-19 positive users

If the authority finds that some of **Bernard**'s PET tokens are present in this list, the authority computes a "risk score", depending in particular on how many PET tokens are present in the list, hence how many users diagnosed with COVID-19 **Bernard** has been in proximity with (and possibly other information, such as exposure duration and a distance estimation). The authority then responds to **Bernard**'s request by informing him about his risk of being exposed to COVID-19.

Security and Privacy benefits of DESIRE

The major advantage of a PET token is the generation of a secret that is shared only between the two applications that were in close proximity. The use of two different PET token lists, “Declare” for infected user declaration and “Status” for exposure status request, ensures several security and privacy properties for the users of DESIRE protocol.

First, while **Alice** and **Bernard** are healthy, **Alice**’s and **Bernard**’s applications provide different tokens from their “Status” lists to request their exposure status (blue token for **Alice** and orange token for **Bernard**). *The central authority is not able to deduce that* ***Alice*** *and* ***Bernard*** *have been in proximity to each other since these blue and orange tokens are unlikable.*

Second, consider the case when **Alice**’s application requests her exposure status using a blue token from her “Status” list and then she is diagnosed COVID-19 positive. To declare her encounters, **Alice**’s application communicates her orange token from “Declare” list. *The central authority is not be able to infer that the two tokens, orange and blue, belong to the same user* ***Alice****.*

To conclude, the use of *“Private Encounter Tokens” (PETs)* and the use of *two PET token lists per application* guaranty a high level of privacy to DESIRE. Moreover, together with a systematic encryption of each database entries in the server, the decryption keys being kept by the clients, DESIRE also features a high resilience to risks of data leaks by the server.