Privacy Preserving Protocol

Introduction

Preserving privacy of personal data is of paramount importance. Most users expect to keep all the data locally and reveal them to a database only if they remain completely anonymous. Our contact tracing module addresses these concerns and beyond that.

Method

Our method is based on DP-3T (available at https://github.com/DP-3T), which is an improved version of the european protocol PEPP-PT (https://www.pepp-pt.org/). We simplified the DP3 protocol to exclude the health agency to authenticate diagnoses from the system, since we have not yet established this connection. This method is completely decentralized, GDPR-compliant, and scalable. In particular, as explained in the DP-3T documentation, this method addressed Article 25 and the EDPB Statement on GDPR and COVID-19.

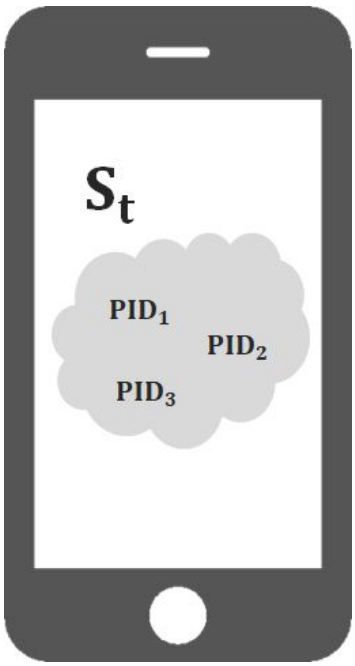
Components:

- Everyday, a secret key S_t is generated on the device using a hash function.

$$S_t = H(S_{t-1})$$

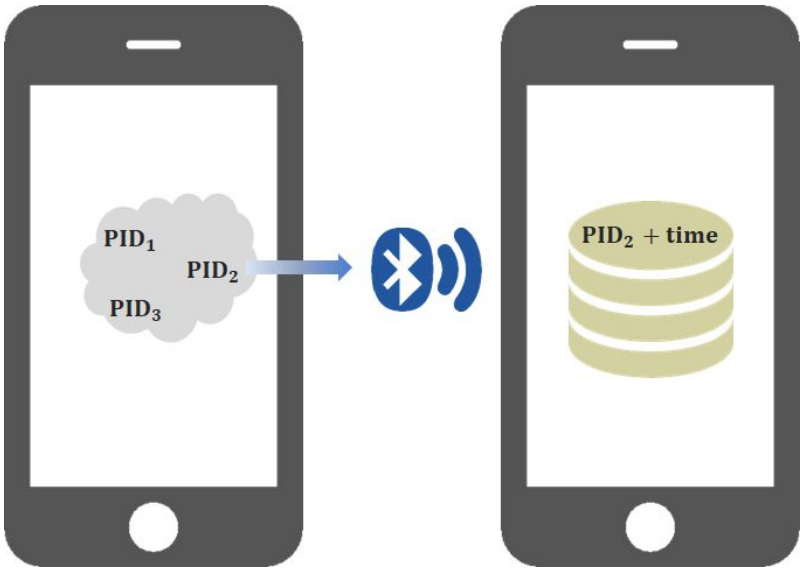
- The secret key generates n p2p IDs (PID):

$$PID_1, PID_2, \ldots = F(S_t)$$



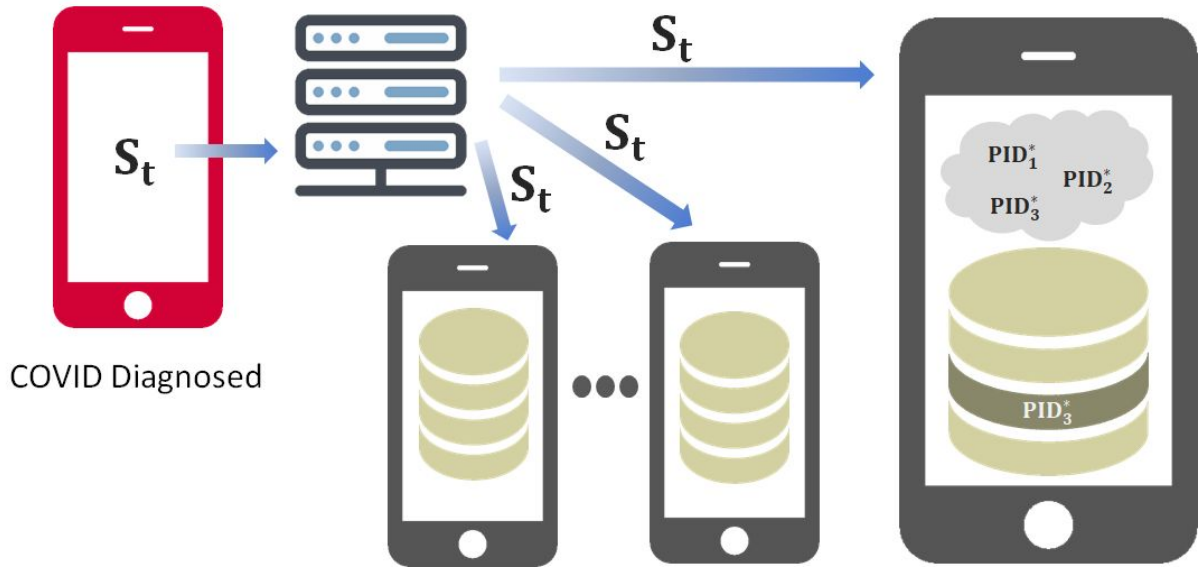
Routines:

- Every 5 minutes, the device selects one PID at random and broadcasts it via Bluetooth
- The phones in the close proximity will receive the signal, store locally on the device PID and contact duration, and add a time and regional tags. No information will be sent to the cloud or leave the phone, except PID which has no personal information.
- The records older than 21 days would be expired and deleted from the records.



COVID-19 diagnose:

- In case a user is diagnosed with COVD-19, the secret key S_t is sent to the server and updates automatically the secret key to preserve the anonymity.
- The server broadcasts the key S_t to **all users.**
- Each user generates all PID using the received secret key. Then it searches in the record to find a match on the device's record.
- If a match is found, the user risk is updated on the device.



Preserved privacy:

- Compatible with **GDPR** Statement on the processing of personal data.
- Only the individuals need to know they are infected.
- To improve privacy, the app generates a secret key every day.
- The contact records are stored only on the device and the server would **never** store it.
- Using the second security level (PID) prevents inference of the contacted people.
- The two-layered security in this method makes it nearly impossible to track a person.
- Using the second security level (PID) prevents a curious user from learning who is infected.
- The server is only used as a channel to broadcast and will not process any information.

Privacy legislation

Here are some concerns that will need to be addressed in order to assert compliance with relevant privacy legislation, i.e. the General Data Protection Regulation (GDPR) of the European Union. Potential specificities of national (Swedish) legislation, such as the age of valid consent to processing of information provided by minors, have not been considered here.

General provisions

The project involves automatic processing of personal data by a controller established in an EU member state, which is within the scope of the GDPR according to Art. 2(1) and Art. 3(1).

Principles

In the general case, the processing of personal data takes place on the grounds that the data subject has given consent to it in accordance with point (a) of Art. 6(1).

Some processing may involve prolonged storage of personal data, thereby giving the data subject time to withdraw consent already given according to Art. 7(3).

Other processing is instantaneous in nature, meaning that the data subject is provided with an immediate response, after which the data is irrevocably anonymized and retained by the controller for the benefit of the public. As the controller no longer has any means of identifying the data subject, the processing of personal data has effectively ceased even before the data subject decides to withdraw consent to this processing.

As the controller may not know the identity of the data subject, verifying that the data subject has reached the required age to give independent consent to the processing may be difficult, or even impossible. The practical implications may be limited, but the issue should be considered further.

As some of the data processed concerns the health of the data subject, this processing requires the data subject to give consent according to point (a) of Art. 9(2).

In most cases, knowing the real world identity (such as name or residential address) of the data subject isn't necessary for the processing, wherefore this information isn't even collected. The only information retained that could be used to pinpoint the location of the data subject is a postal zip code, which typically is the same for hundreds or thousands of individuals, thereby

effectively anonymizing the information. In these cases, in accordance with Art. 11(2) the controller will be exempt from the obligations implied by Art. 15-20.

Rights of the data subject

As personal information is obtained electronically from the data subject, information about the processing will be made available in that context according to Art. 13.

The rights stipulated by Art. 15-20 will have to be addressed only to the extent the controller in each case knows the identity of the data subject, due to the provisions in Art. 11(2).

Controller and processor

As stipulated in Art. 25, data minimisation and pseudonymisation are important measures taken to meet the requirements of the GDPR.

A written specification of the processing activities should be produced by the controller according to Art. 30.

Security measures according to Art. 32 are being chosen to reduce the risk of violating the rights of the data subject.