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 DP3 (available at https://github.com/DP-3T), which is an improved version of the european protocol PEPPT (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.

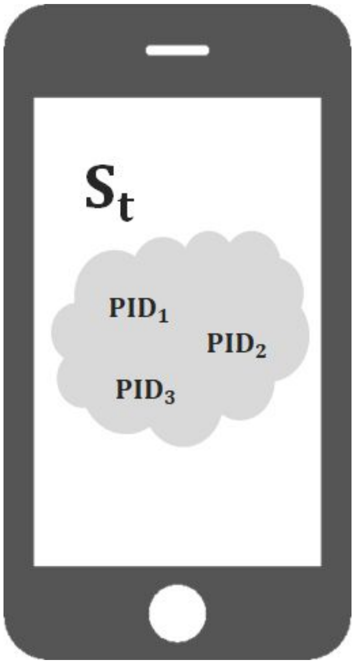
Components:

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

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

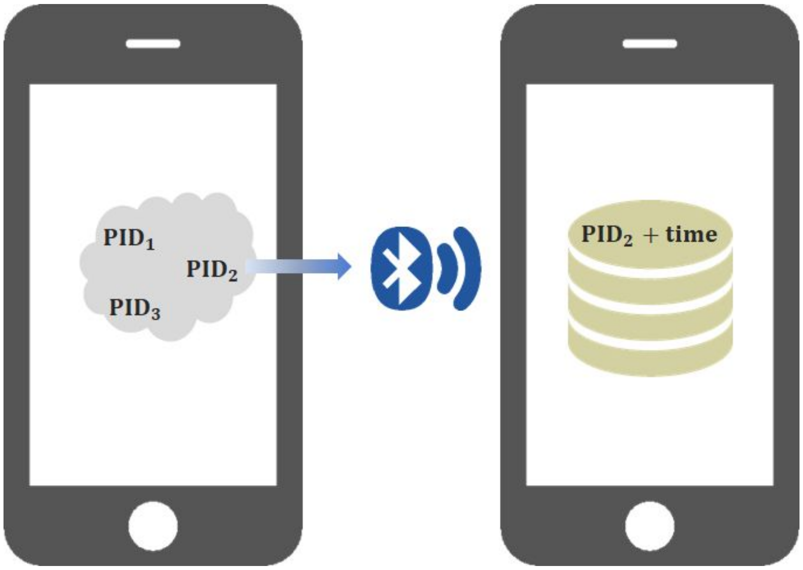
- The secret key generates n p2p IDs (PID):

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



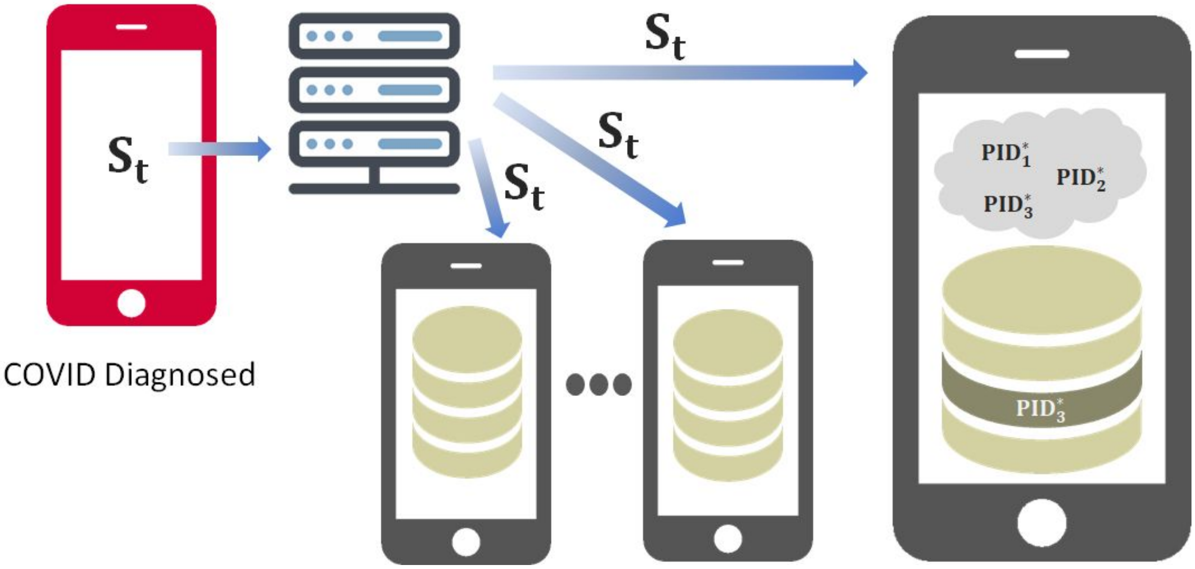
Routines:

- 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.