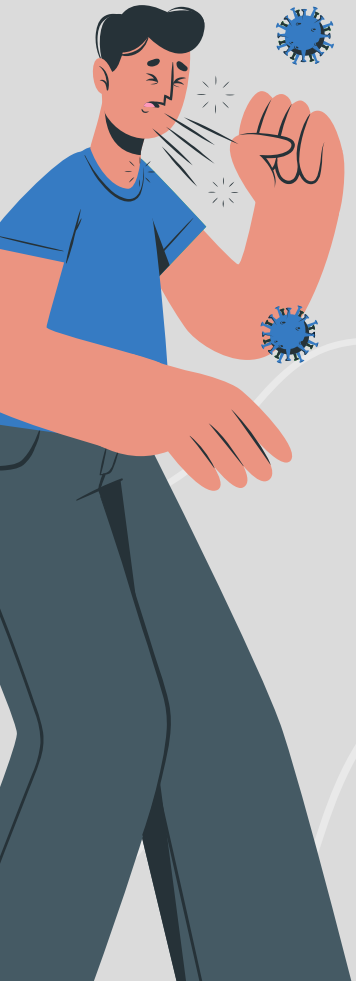


Contact Tracing

Tracking potential COVID-19 contamination

Grupo 04

Matheus Franco 92523; Tiago Fournigault 92562; Guilherme Gaspar 102335

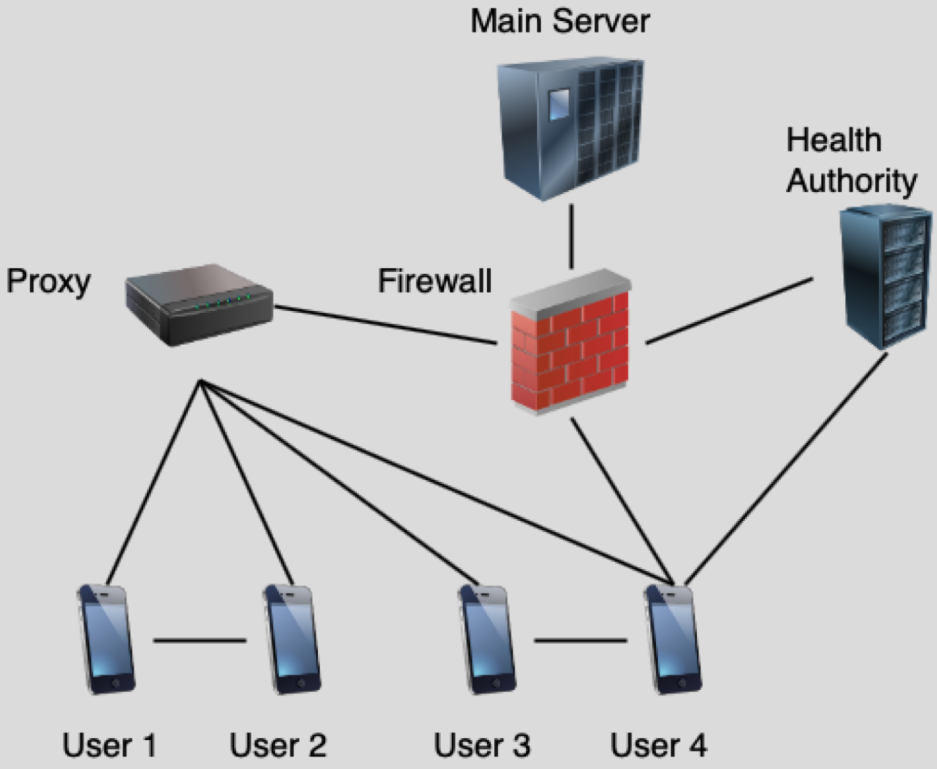
Introduction

- The goal of this project is to identify potential contamination of COVID-19 based on user social interaction.
- At the same time that it is affected by the person's whereabouts and daily routines, the application must maintain the privacy of each user.

The app should:

- inform others that the user is infected (using a code given by a health authority) and
- Inform the user if he was in contact with someone infected, alongside with an description of where the contact occurred and its time.

General Architecture



- Main server (+ firewall)
- Proxy
- Health Authority
- Users

Key Distribution and Management

- Each entity has its own public and private key alongside with a certificate, which is assumed to be signed by a Certificate Authority.
- The public keys of the main server, the proxy and the sns (Health Authority) are previously known. For each user, on the other hand, it's generated in the beginning of the execution by the app.

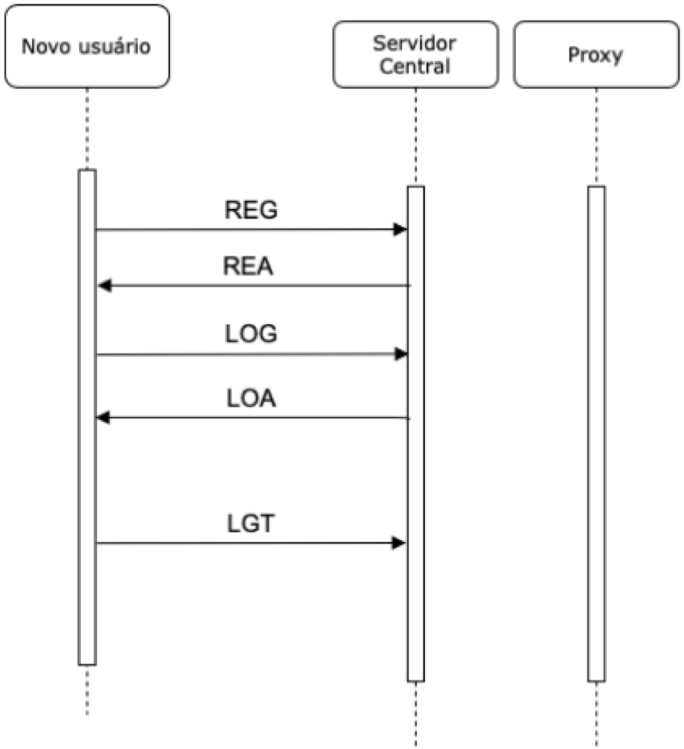
```
os.system("openssl genrsa -out " + key + " > /dev/null 2>&1")
os.system("openssl rsa -in "+ key + " -pubout > " + public_key + " > /dev/null 2>&1")
os.system("echo -e \"\n\n\n\n\n\n\n\n\n\n\" | openssl req -new -key " + key + " -out " + cert + " > /dev/null 2>&1")
os.system("openssl x509 -req -days 365 -in " + cert + " -signkey " + key + " -out " + cert + " > /dev/null 2>&1")
```

Generation of keys and certificate

Developed Protocol

User Registration and log in:

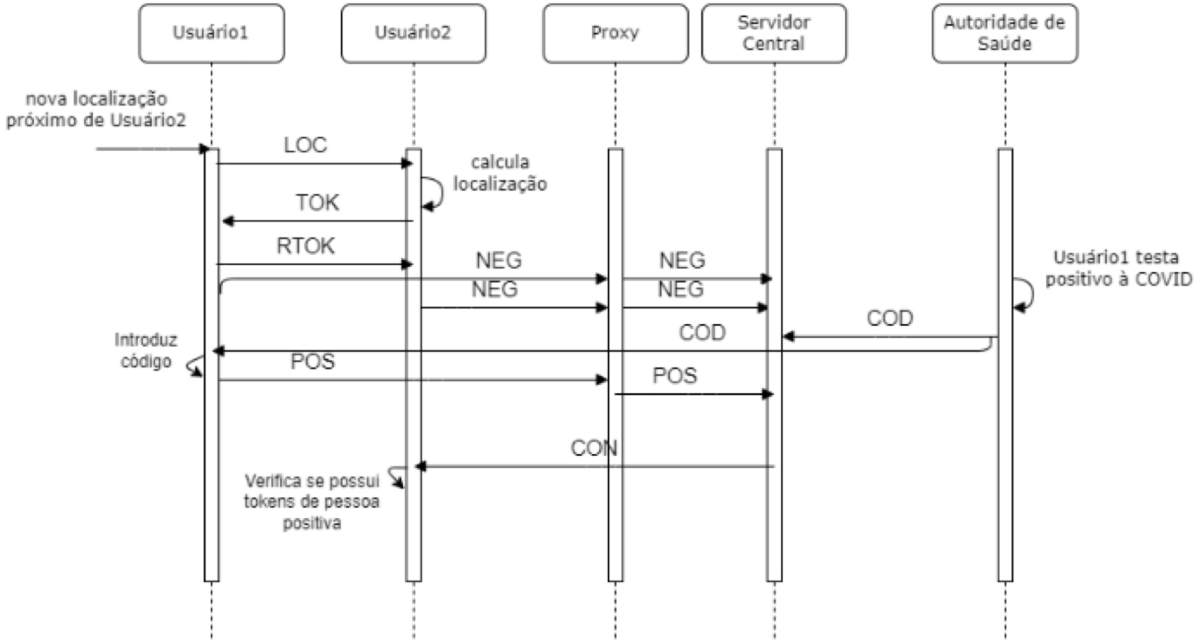
- REG:<name>:<password>:\n
- REA:\n
- LOG:<password>:\n
- LOA:(<logged_ip>:)*\n
- LGT:\n



Developed Protocol

Social interaction:

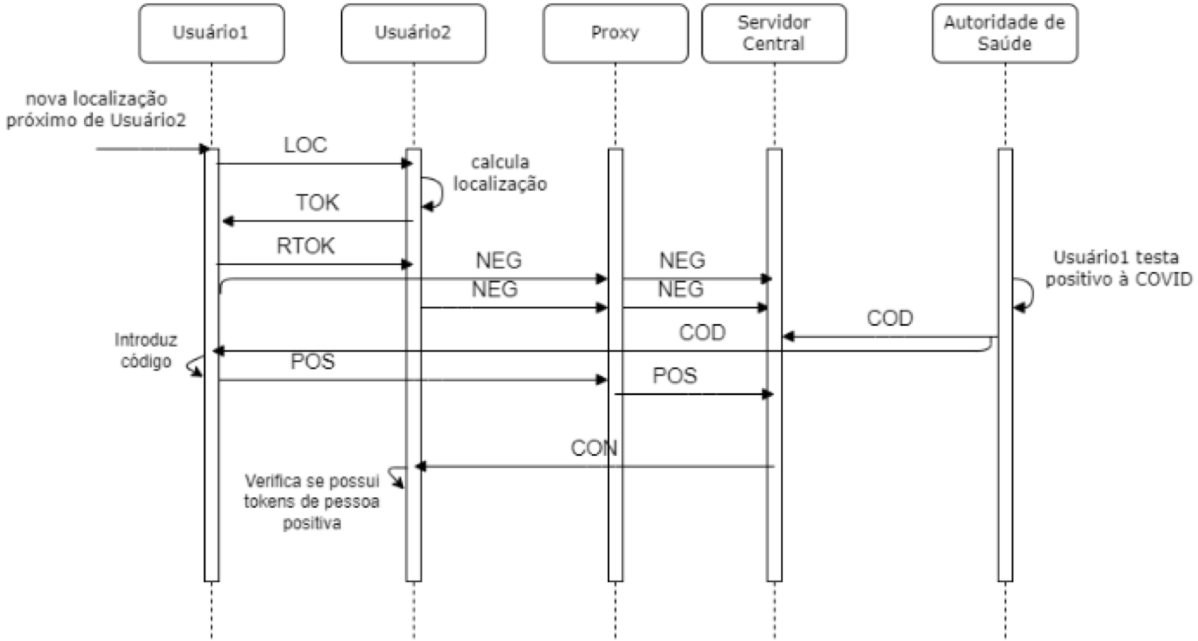
- LOC:<latitude>:<longitude>:\n
- TOK:<mytoken>:\n
- RTOK:<mytoken>:\n



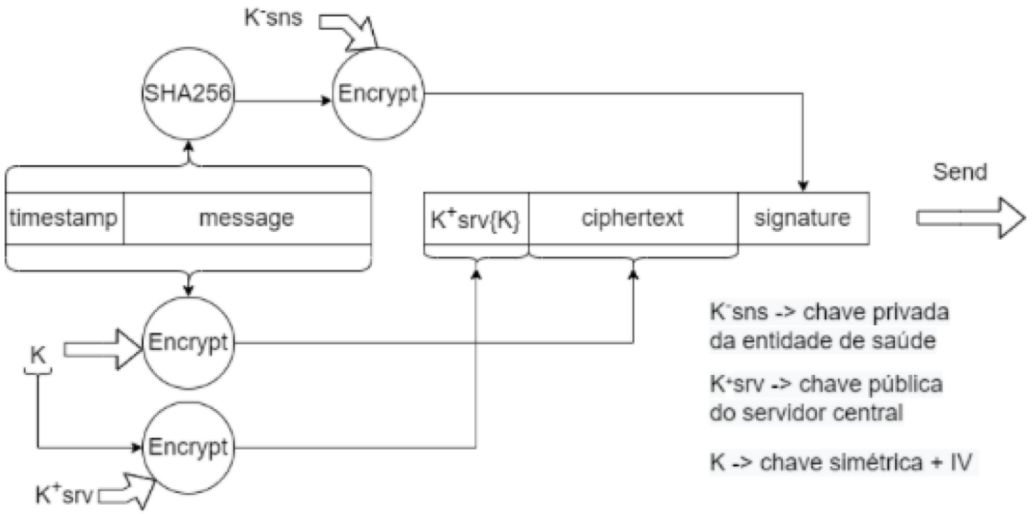
Developed Protocol

Positive test:

- COD:<sns_code>:\n
- POS:<sns_code>:(<token>:)*\n
- CON:(<token>:)*\n
- NEG:\n

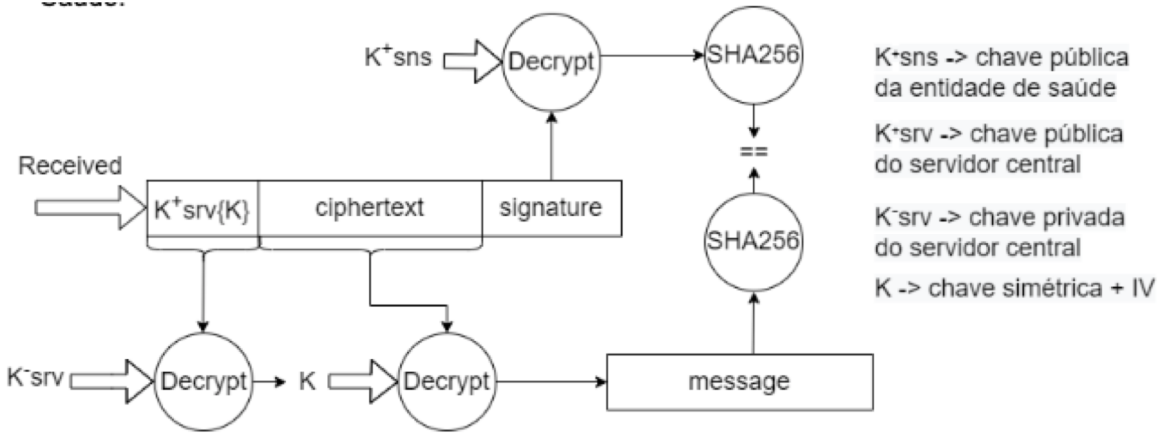


Developed Protocol



Positive test (sns to server message)

Developed Protocol



Positive test (sns to server message)

References:

D3PT - Decentralized Privacy-Preserving Proximity Tracing
(https://github.com/DP-3T/documents)

Apple and Google Privacy-Preserving Contact Tracing - joint documentation from the two leading smartphone OS providers.
(https://covid19.apple.com/contacttracing)

Project Description (https://github.com/tecnico-sec/Project-Topics-2022_1)

Slides from theoretical classes
(https://fenix.tecnico.ulisboa.pt/disciplinas/SIRS/2021-2022/1-semestre/teoricas)