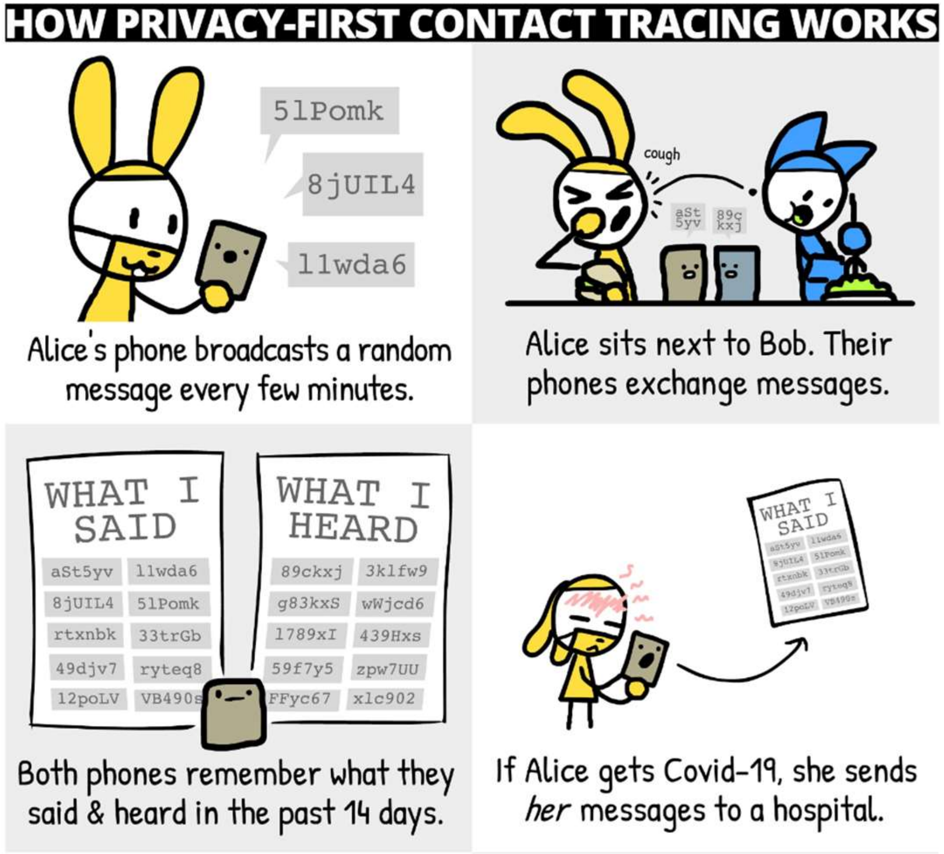
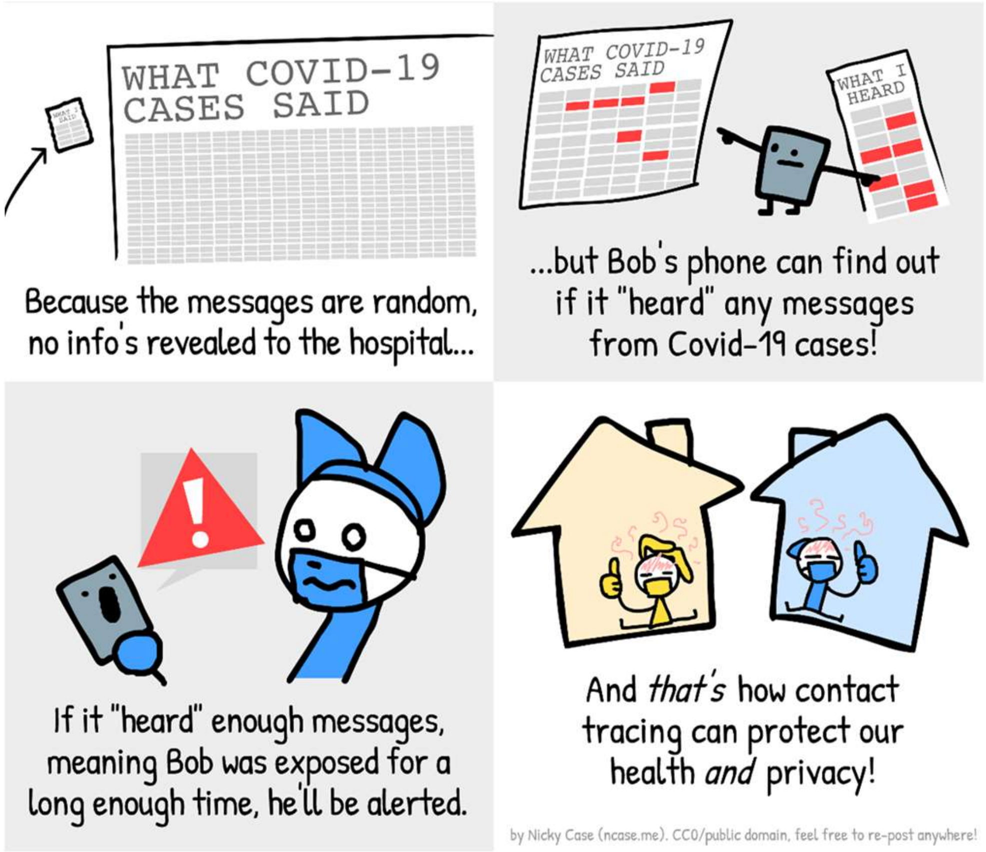
# A28-CT

Group 28:

- Afonso Gomes
- António Martins
- Miguel Henriques

# Overview


HOW PRIVACY-FIRST CONTACT TRACING WORKS
51Pomk
8jUIL4
11wda6
Alice's phone broadcasts a random message every few minutes.
cough
aSt5yv
89ckxj
Alice sits next to Bob. Their phones exchange messages.
WHAT I SAID
aSt5yv 11wda6
8jUIL4 51Pomk
rtxnbk 33trGb
49djv7 ryteq8
12poLV VB490s
WHAT I HEARD
89ckxj 3klfw9
g83kxS wWjcd6
1789xI 439Hxs
59f7y5 zpw7UU
FFyc67 xlc902
Both phones remember what they said & heard in the past 14 days.
WHAT I SAID
If Alice gets Covid-19, she sends *her* messages to a hospital.


WHAT I SAID
WHAT COVID-19 CASES SAID
Because the messages are random, no info's revealed to the hospital...
WHAT COVID-19 CASES SAID
WHAT I HEARD
...but Bob's phone can find out if it "heard" any messages from Covid-19 cases!
If it "heard" enough messages, meaning Bob was exposed for a long enough time, he'll be alerted.
And *that's* how contact tracing can protect our health *and* privacy!

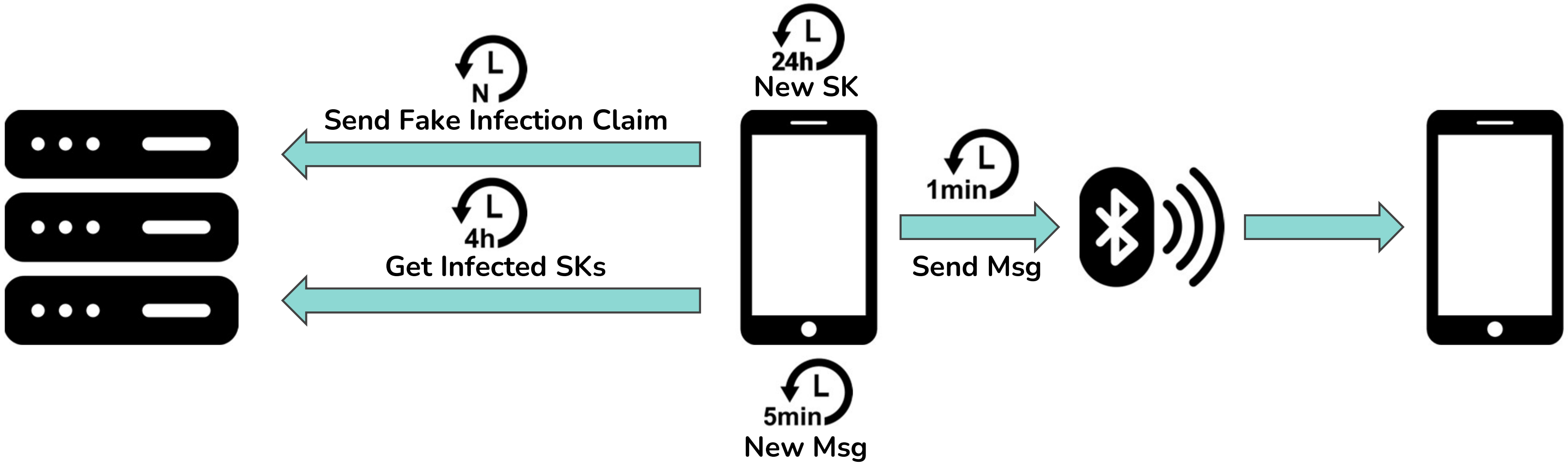
by Nicky Case (ncase.me). CC0/public domain, feel free to re-post anywhere!

https://ncase.me/contact-tracing/

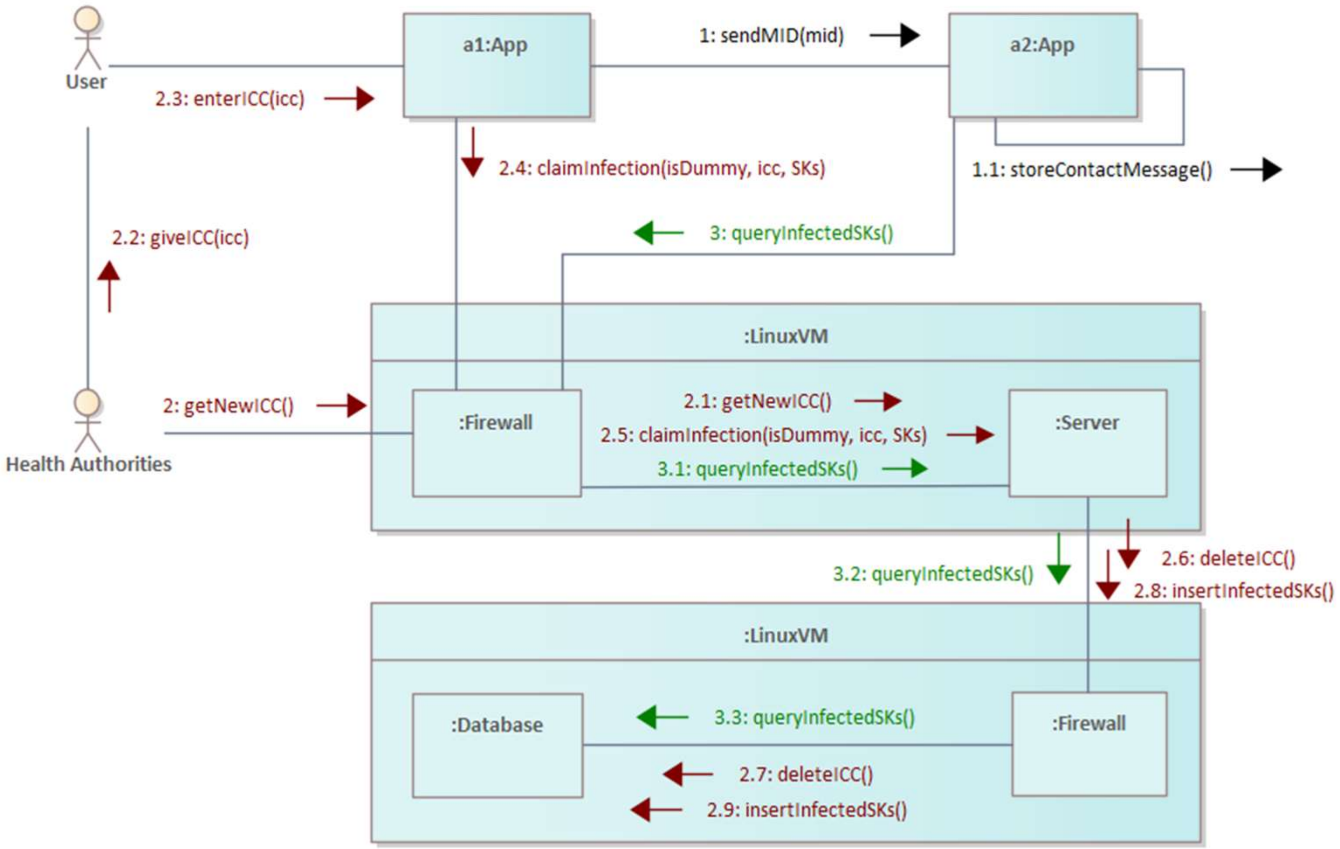
# Demonstration

https://youtu.be/LOqResw_ZKQ

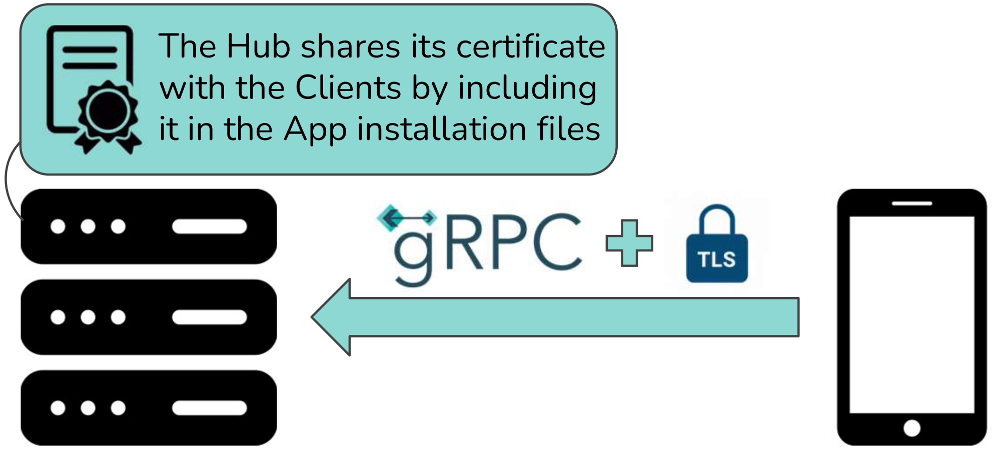
# App Background Activity



# Communication Diagram



# Key Distribution



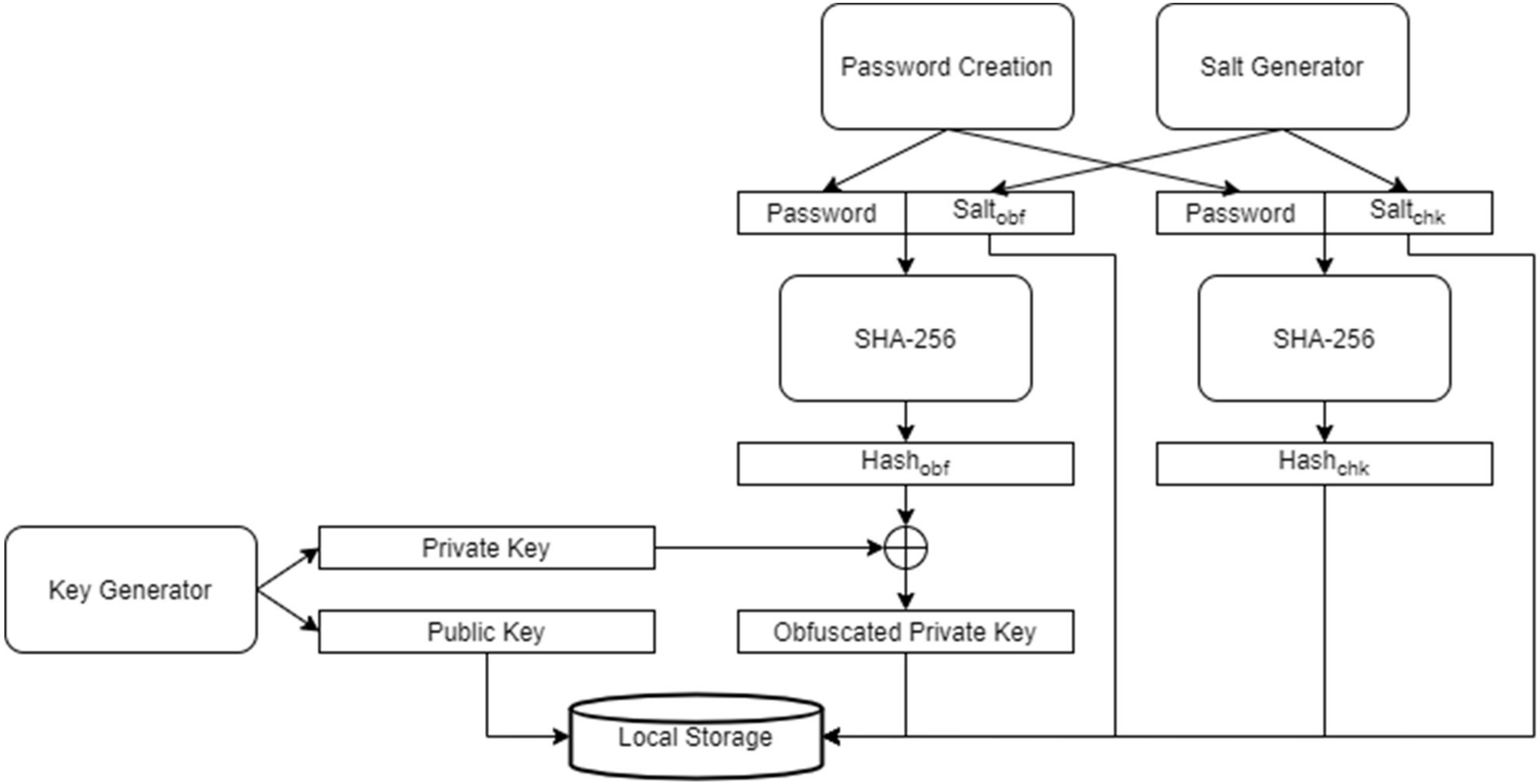
The Hub shares its certificate with the Clients by including it in the App installation files

In a real deployment of the system, it would be much more secure to register the Hub's certificate with a trustworthy Certification Authority.

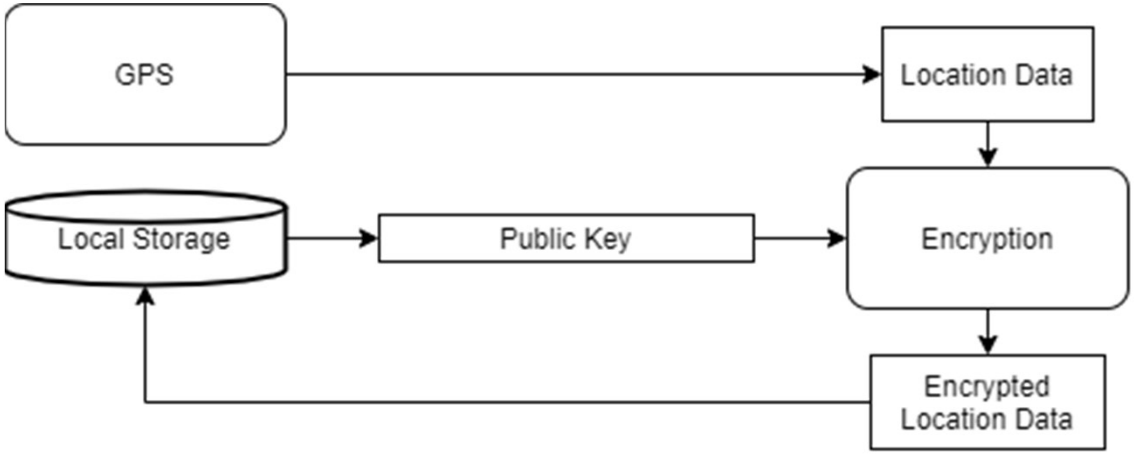
Also regarding the verification of the Hub's certificate, we have disabled the hostname verification as we do not have a stable hostname assigned to the Hub. However, it would be more secure to acquire a stable hostname and enable hostname verification.

# Custom Protocol: Secure Storage of Location Data

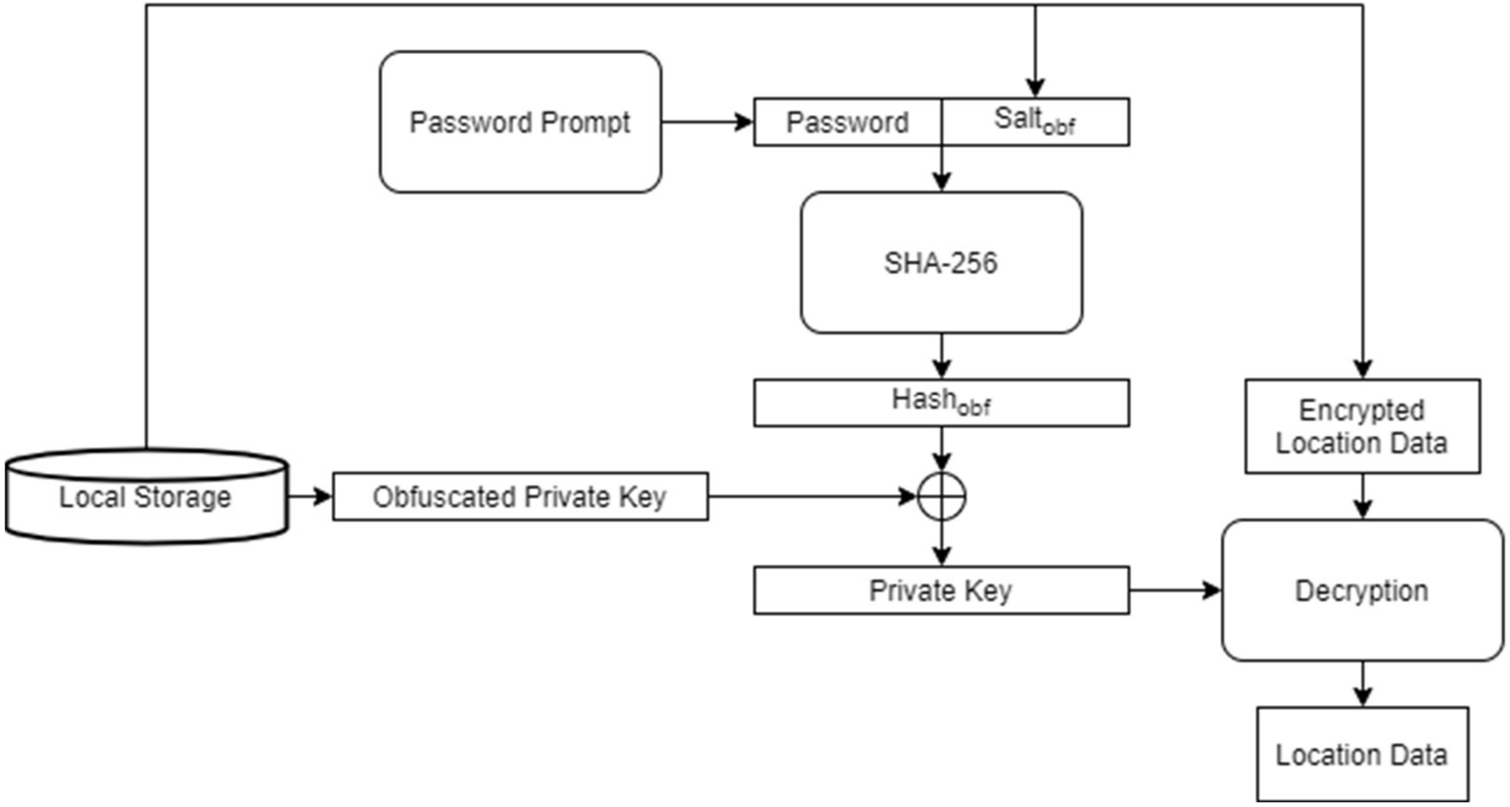
# Initial Setup



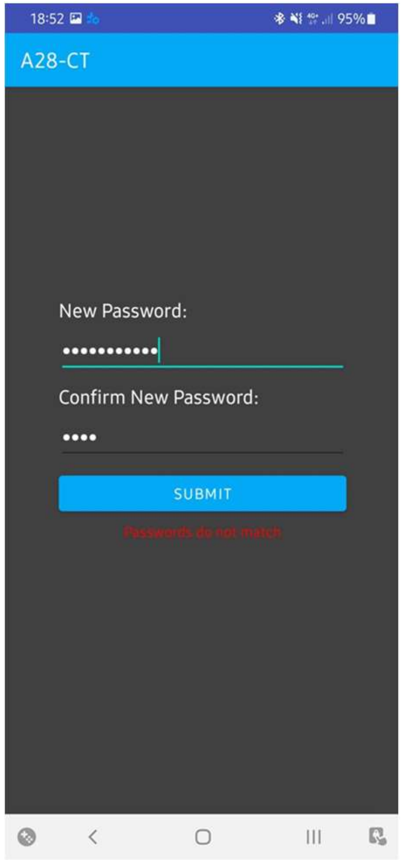
# Encryption of Location Data



# Decryption of Location Data



# Password Input



A28-CT

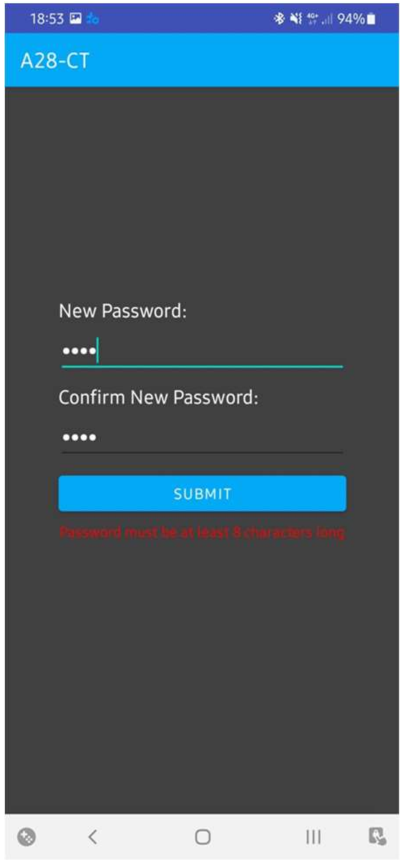
New Password:

•••••••••••

Confirm New Password:

••••

Passwords do not match



A28-CT

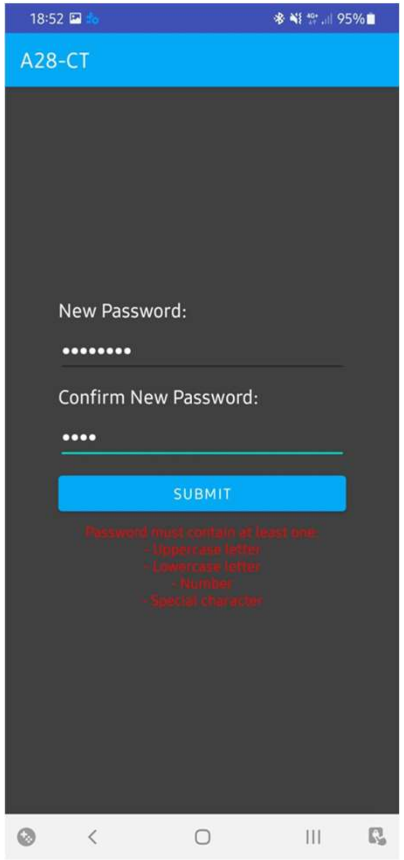
New Password:

••••

Confirm New Password:

••••

Password must be at least 8 characters long



A28-CT

New Password:

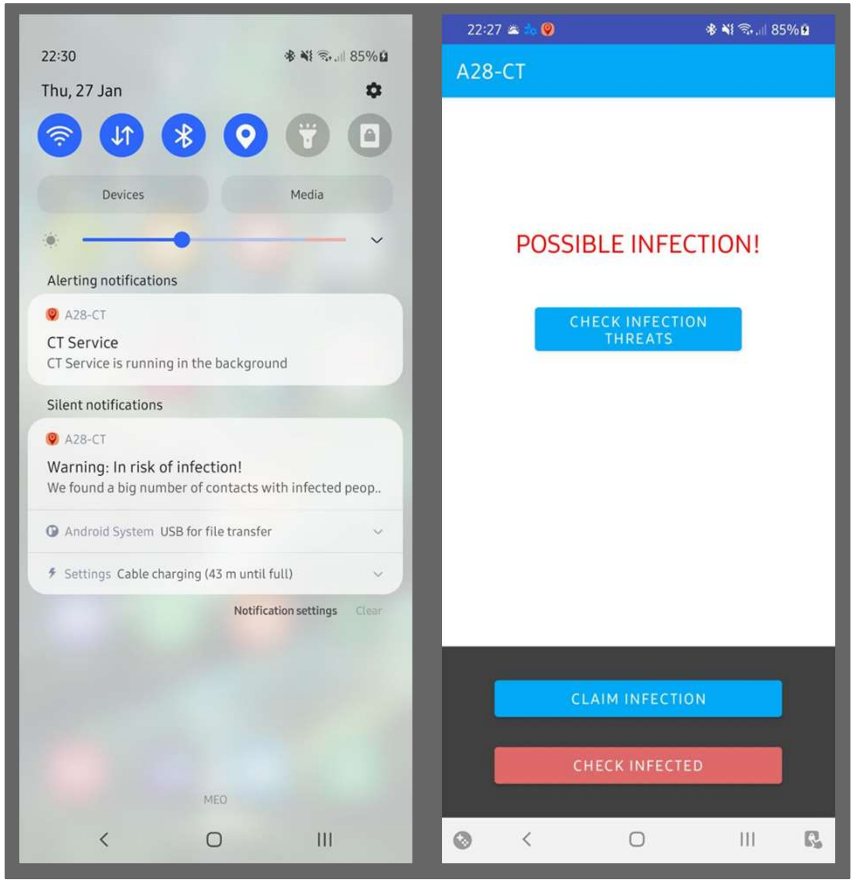
••••••••

Confirm New Password:

••••

Password must contain at least one:
- Uppercase letter
- Lowercase letter
- Number
- Special character

# Use Password To See Contact Information



Alerting notifications

A28-CT

CT Service

CT Service is running in the background

Silent notifications

A28-CT

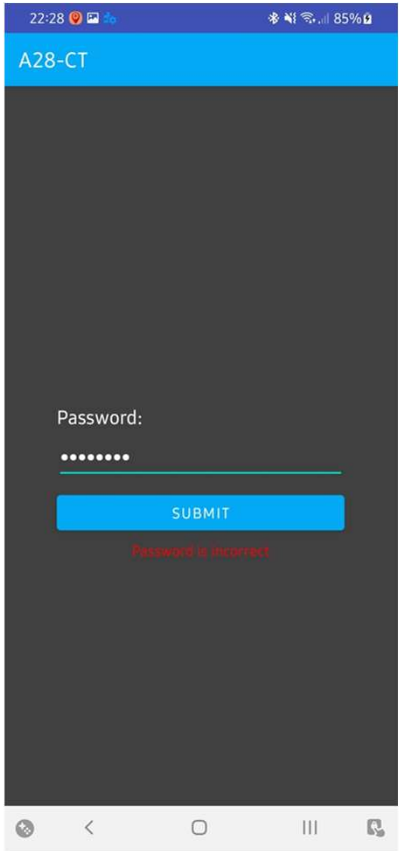
Warning: In risk of infection!

We found a big number of contacts with infected peop..

Android System USB for file transfer

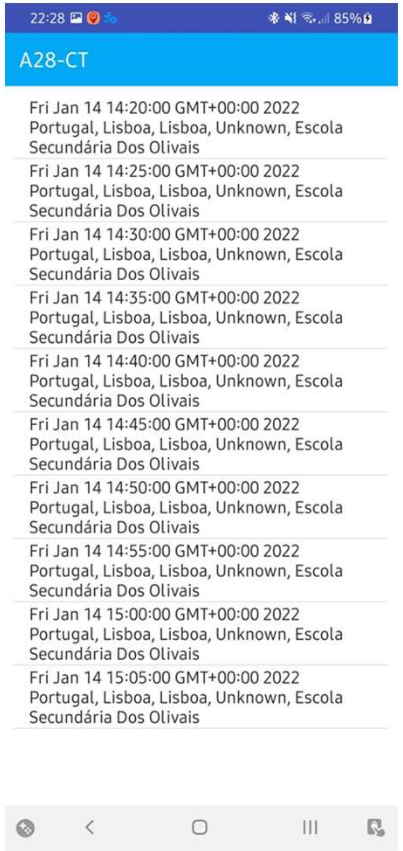
Settings Cable charging (43 m until full)

POSSIBLE INFECTION!



Password: ••••••••

Password is incorrect



Fri Jan 14 14:20:00 GMT+00:00 2022 Portugal, Lisboa, Lisboa, Unknown, Escola Secundária Dos Olivais

Fri Jan 14 14:25:00 GMT+00:00 2022 Portugal, Lisboa, Lisboa, Unknown, Escola Secundária Dos Olivais

Fri Jan 14 14:30:00 GMT+00:00 2022 Portugal, Lisboa, Lisboa, Unknown, Escola Secundária Dos Olivais

Fri Jan 14 14:35:00 GMT+00:00 2022 Portugal, Lisboa, Lisboa, Unknown, Escola Secundária Dos Olivais

Fri Jan 14 14:40:00 GMT+00:00 2022 Portugal, Lisboa, Lisboa, Unknown, Escola Secundária Dos Olivais

Fri Jan 14 14:45:00 GMT+00:00 2022 Portugal, Lisboa, Lisboa, Unknown, Escola Secundária Dos Olivais

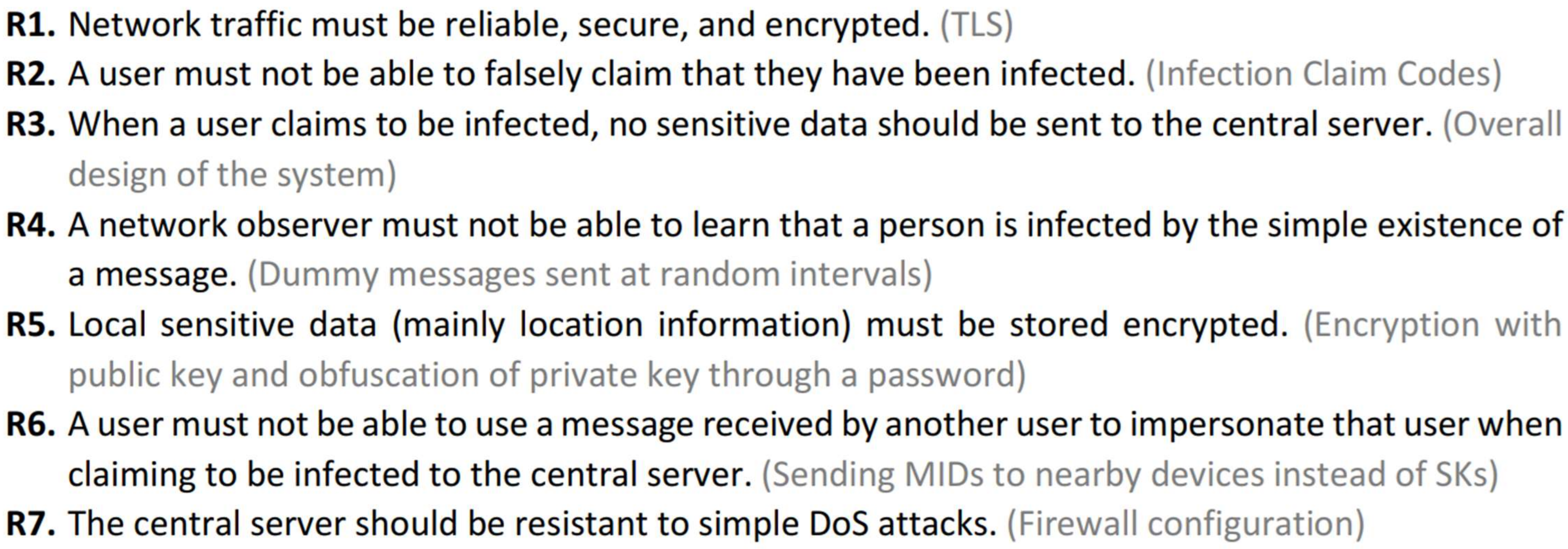
Fri Jan 14 14:50:00 GMT+00:00 2022 Portugal, Lisboa, Lisboa, Unknown, Escola Secundária Dos Olivais

Fri Jan 14 14:55:00 GMT+00:00 2022 Portugal, Lisboa, Lisboa, Unknown, Escola Secundária Dos Olivais

Fri Jan 14 15:00:00 GMT+00:00 2022 Portugal, Lisboa, Lisboa, Unknown, Escola Secundária Dos Olivais

Fri Jan 14 15:05:00 GMT+00:00 2022 Portugal, Lisboa, Lisboa, Unknown, Escola Secundária Dos Olivais

# Security Requirements



**R1.** Network traffic must be reliable, secure, and encrypted. (TLS)

**R2.** A user must not be able to falsely claim that they have been infected. (Infection Claim Codes)

**R3.** When a user claims to be infected, no sensitive data should be sent to the central server. (Overall design of the system)

**R4.** A network observer must not be able to learn that a person is infected by the simple existence of a message. (Dummy messages sent at random intervals)

**R5.** Local sensitive data (mainly location information) must be stored encrypted. (Encryption with public key and obfuscation of private key through a password)

**R6.** A user must not be able to use a message received by another user to impersonate that user when claiming to be infected to the central server. (Sending MIDs to nearby devices instead of SKs)

**R7.** The central server should be resistant to simple DoS attacks. (Firewall configuration)