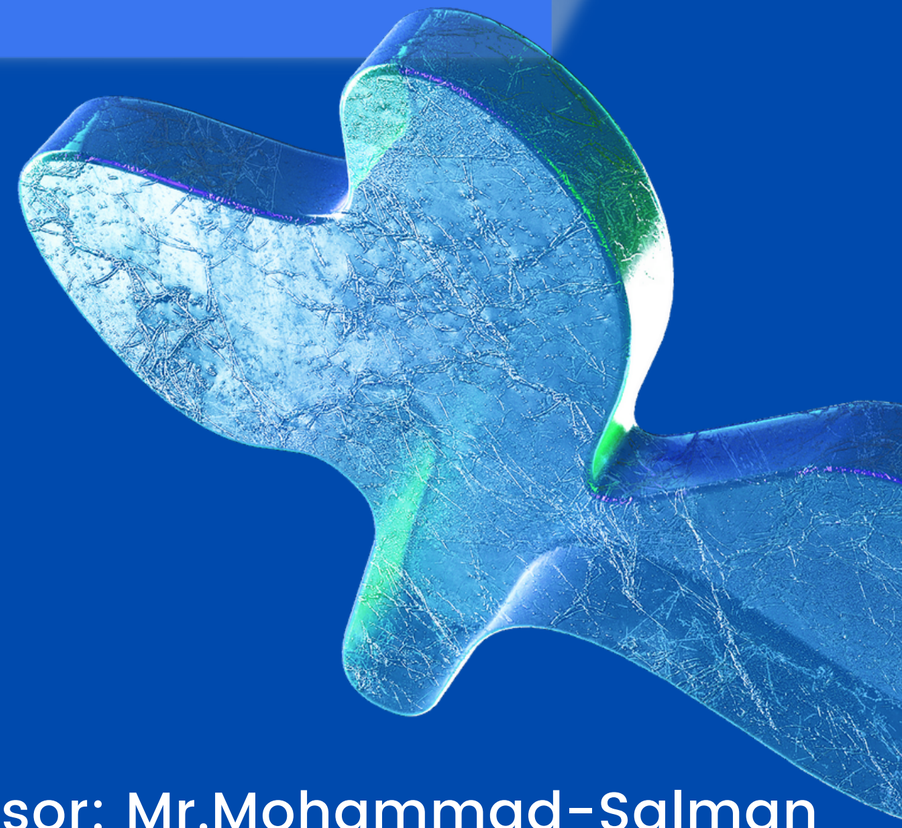
GROUP
PRESENTATION

Data Privacy by Design



GROUP 11 DATE:11th May 2022

GROUP MEMBERS : Ruthvik Ravish | Yuanyuan LIU | Haozhe TANG | Sanujan Thavarasa | Malek Zannad

Professor: Mr.Mohammad-Salman Nadeem

Introduction of Signal

1

In February 2014, Open Whisper Systems introduced Signal to provide private chatting and internet calling with end-to-end encrypted security.

2

The keys are generated and stored on the phones but not on the servers. As to secure the privacy of the user messages.

3

Signal is said to be safer than most of the messaging apps as it utilizes state-of-the-art security which ensures that no one and not even the developers of Signal to intercept and read the messages.

4

Signal allows its users to set timers to automatically delete messages within certain period.

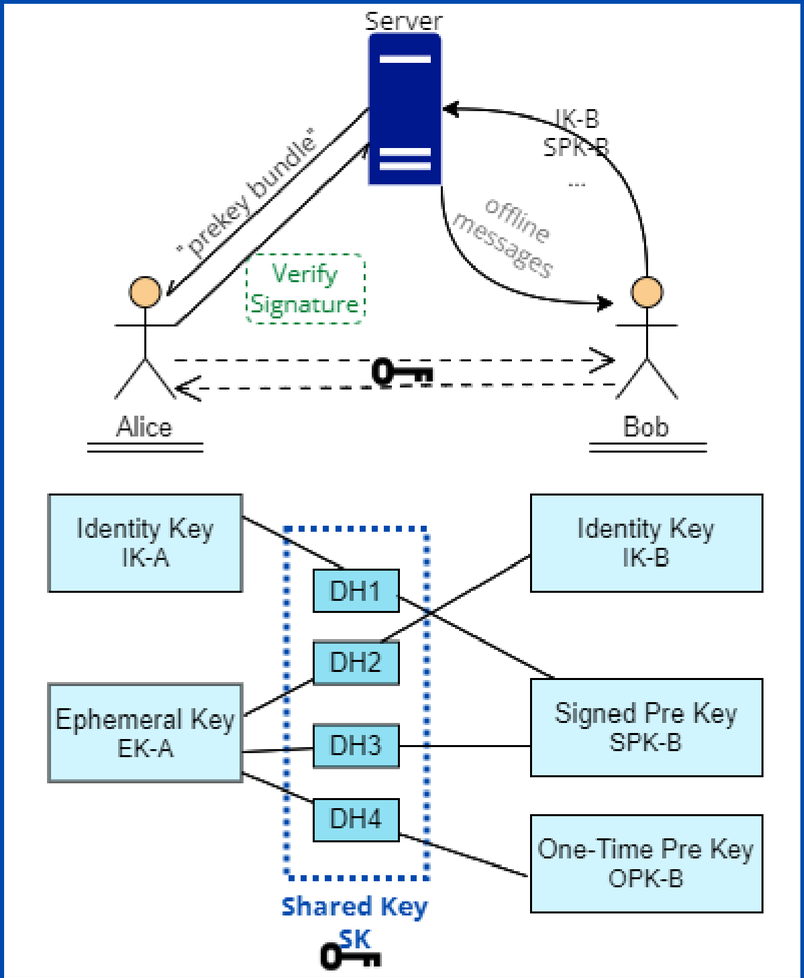
5

Signal software is free and its licence for mobile clients is GPL-3.0 and for desktop it uses AGPL-3.0. The complete source code is available for the users on GitHub.

6

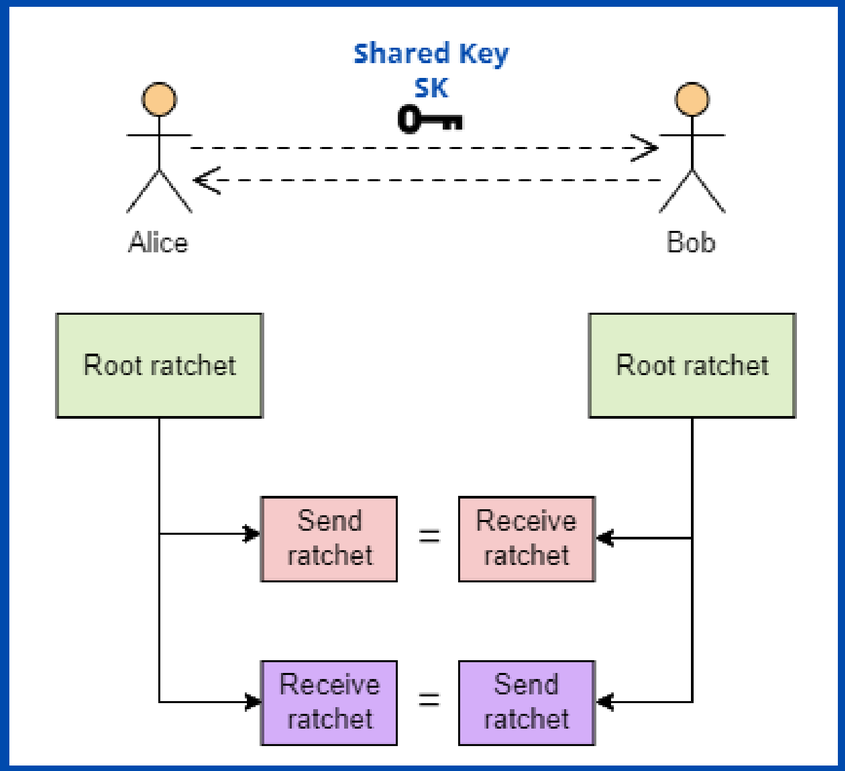
Includes a cryptocurrency wallet for users to store, send and receive in-app payments.

X3DH + Double Ratchet



+

symmetric-key ratchet & DH ratchet

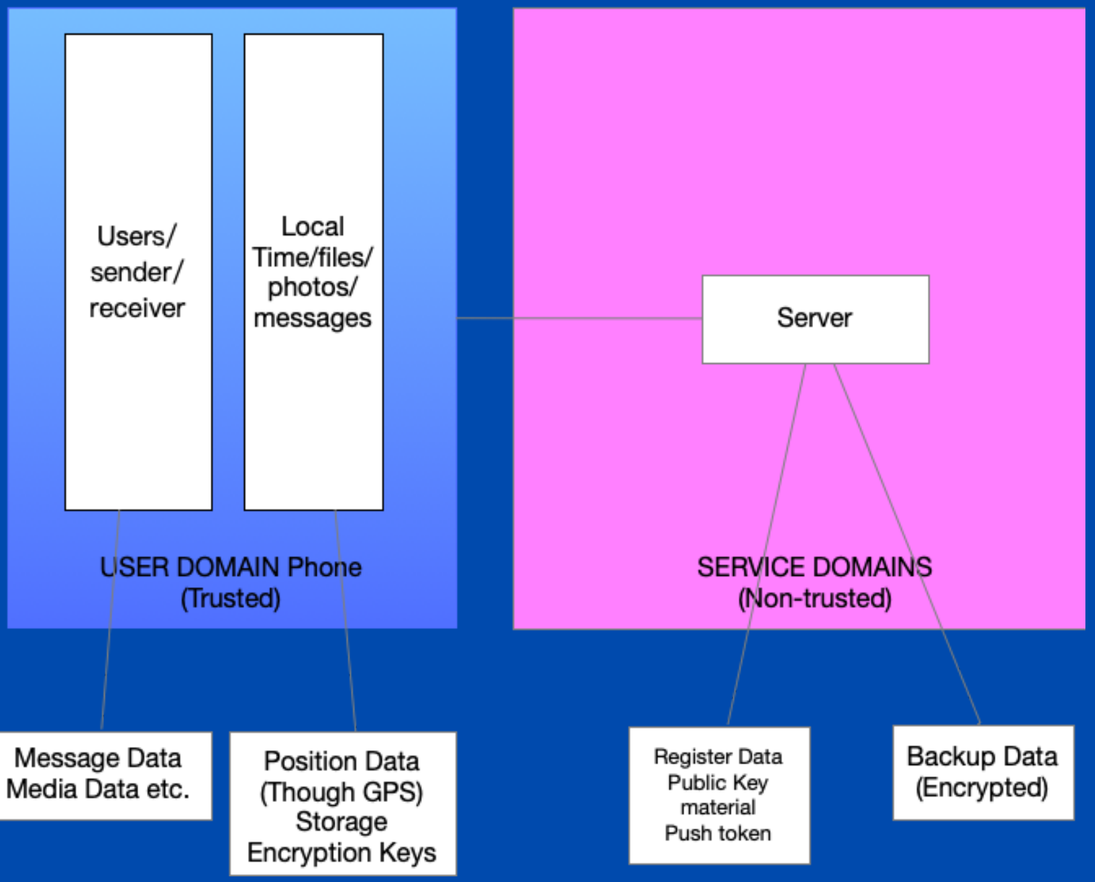


Alice and Bob use X3DH to agree on a shared key. Then they can send and receive encrypted messages using the Double Ratchet algorithm.

... + XEdDSA & VXEdDSA + Sesame

Activity 1-3

1st activity

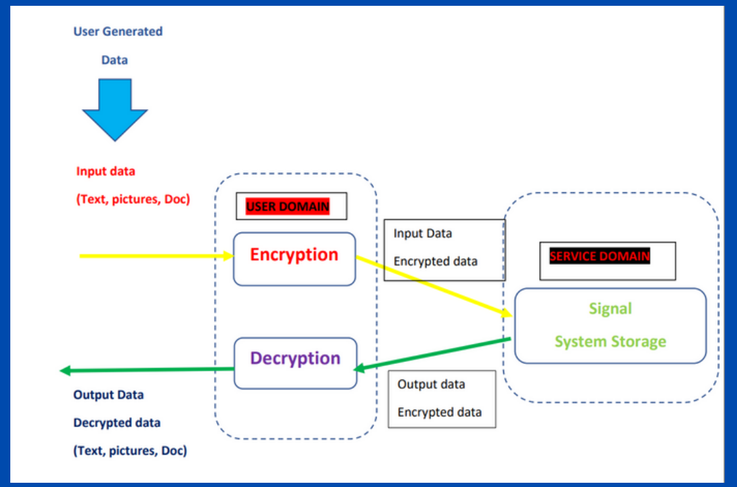


2nd activity

Signal app collects only the phone number of the users for them to access to the application.
Personal information is optional for users to provide.

Personal data(phone number) -- to get registered
Encrypted password-- to get registered
Location/Contacts/Storage etc.-- Optional
Temporary Saving on server--when receiver is not online.

3rd activity



Distribution of the data between domain is starting from user domain, it is taking user data as input and processing into meaning full output information where service domain will capture those data as an input data and processing in to fulfill the functionality.

Activity 4 :

- Elements recquired

Signal's security model is based on a trusted third party

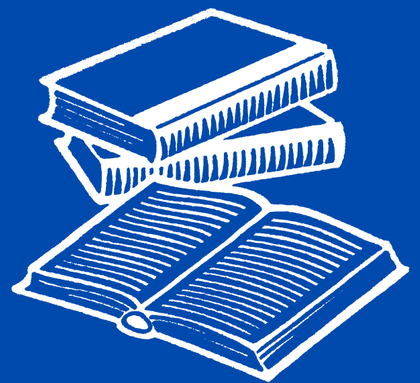
ITelephone register
The system works under this reserve of trust

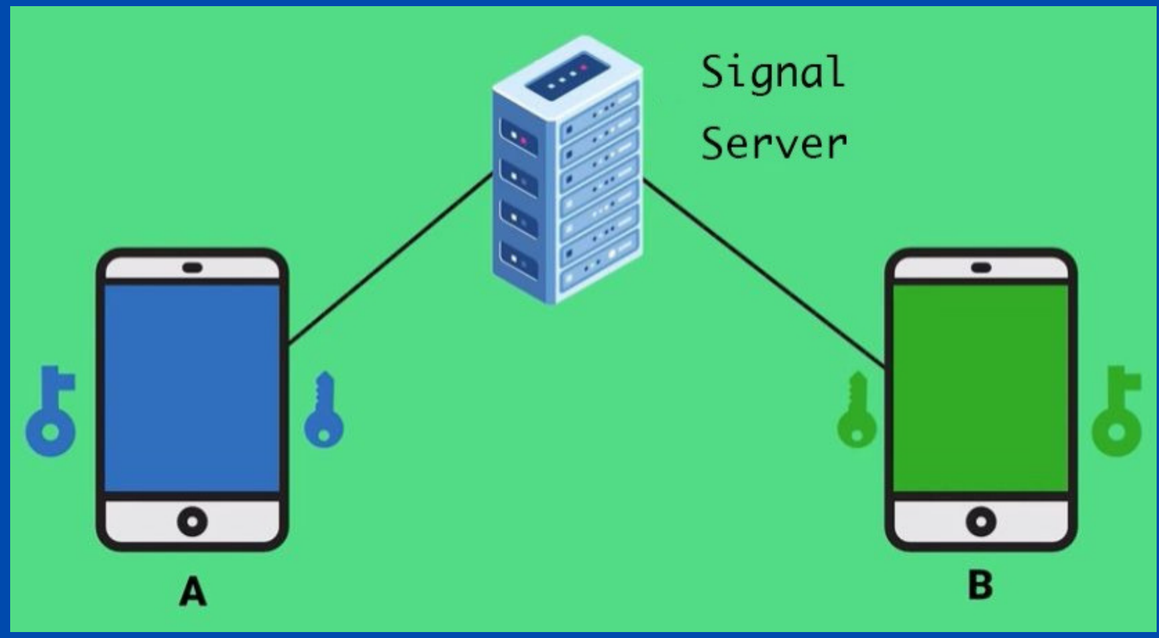
No control over it
We have no choice but to give consent to use the application

Like that, Signal has the phone number of every user stored in its server.

We consider phone numbers as sensitive and personnal data.

A possible leak from the server-side could have serious consequences.





- Other informations about signal:

End to end encryption BY DEFAULT

Signal itself does not have your personal key so it cannot decrypt the messages it relays.

It relies on a user key
Every user has a couple of keys.
A public key : used by everyone to send a message to Bob
A private key: Only created and used by Bob's device to decrypt messages sent through his public key

The problem with this is the management of this user key

What happens if I lose my key?
Do I lose access to my data?

The answer is yes
This is the compromise
Keep access to data or have a security guarantee

Activity 4 : What can go wrong? What are the solutions?

- Mass attack vs. targeted attack
- Hacking has become a business
- A targeted attack is not profitable in the case of signal
- Mass attack: I implement something to get access to the source directly.
- Mass attacks are possible only in the case where the data are centralized
- From the moment the data is centralized a mass attack is possible

- It is enough that a person has access to the server to be able to distribute wrong keys to everyone and will then be able to decrypt everyone's exchanges.
- The individual will be able to modify the public keys of people.
- By doing this he will not be able to access the data already on your device but will be able to intercept any new message to decrypt it with his personal key.

Solution that can be proposed:

Max want to have a conversation with Bob.
They exchange a unique digit code/QR code generated foreach conversation.
The code has to be the same to make sure they are both senders and receivers.